Benutzerhandbuch

Modem Pirelli PRG AV4202N

TELE KOM AUS TRIA

Inhaltsverzeichnis

1. Willkommen 4
   - Über dieses Handbuch 4
   - Hinweissymbol 4
   - Textkonventionen 4
2. Einleitung 5
   - Einleitung 5
   - Vorteile des Routers 5
   - Mindestvoraussetzungen für System und Komponenten 6
   - Beispiel für ein Heimnetzwerk 6
   - Vorderseite 7
   - Rückseite 8
3. Installation der Hardware 9
   - Einleitung 9
   - Aufstellen des Routers 9
   - Router einschalten 10
   - Router verbinden 10
4. Installation Ihres Computers 12
   - Ethernet-Verbindung 12
   - Ethernet-Verbindung: Installation des TCP/IP-Protokolls 12
   - Ethernet-Verbindung: MS Windows 98SE, ME, 2000 13
   - Ethernet-Verbindung: MS Windows XP 14
   - Ethernet-Verbindung: MAC OS 10.X 16
   - Wi-Fi-Verbindung 17
5. Konfiguration des Routers 18
   - Einleitung 18
   - Verfügbare Netzwerkobjekte 20
6. Netzwerkverbindungen 21
   - LAN Bridge 21
   - LAN Bridge: Allgemein 21
   - LAN Bridge: Einstellungen 22
   - LAN Bridge: Routing 25
   - LAN Bridge: Bridging 26
   - LAN Ethernet 27
   - LAN Ethernet: Allgemein 27
   - LAN Ethernet: Einstellungen 28
   - LAN Ethernet: Erweitert 28
   - LAN Wireless 802.11n Access Point 28
   - LAN Wireless 802.11nn Access Point: Allgemein 29
   - LAN Wireless 802.11n Access Point: Einstellungen 29
   - LAN Wireless 802.11n Access Point: Wireless (Drahtlos) 30
   - LAN Wireless 802.11n Access Point: Erweitert 34
   - WAN DSL 35

Inhaltsverzeichnis

→ WAN DSL: Allgemein 35
→ WAN DSL: Einstellungen 36
7. Sicherheit 37
→ Allgemein 37
→ Zugriffskontrolle 39
→ Portweiterleitung 40
→ DMZ Host 43
→ Port Triggering 44
→ Webseiten-Einschränkungen 45
→ Verbindungen 46
→ Sicherheitslog 47
8. Erweitert 48
→ Benutzer 49
→ Datum und Uhrzeit 50
→ DDNS 51
→ Diagnose 52
→ Disc-Management 53
→ Druckerserver 54
→ File Server 55
→ FTP Server 55
→ Konfigurationsdatei 56
→ Media Sharing 56
→ PRG AV4202N Firmware Upgrade (Aktualisierung) 57
→ Protokolle 58
→ Sicherung und Wiederherstellung 59
→ Universal Plug and Play 61
→ Wake Up on LAN 61
→ Web Server 62
→ Werkseinstellungen wiederherstellen 63
9. Systemüberwachung 64
→ Network Connections (Netzwerkverbindungen) 64
→ Systemlog 64
→ CPU 65
10. Problembehebung 66
→ Grundlegende Verbindungstests 66
→ Browsen zu den Konfigurationsbildschirmseiten des Routers 66
→ Mit dem Internet verbinden 66
→ Vergessenes Passwort und Zurücksetzen auf Werkseinstellungen 67
→ Drahtlose Vernetzung 67
→ Häufig gestellte Fragen 68
11. Sicherheitshinweise 69
12. IP-Adressierung 70

Inhaltsverzeichnis

- Die Internetprotokollfamilie 70
- Verwaltung des Routers über das Netzwerk 70
- IP-Adressen und Subnetzmasken 70
- Wie erhält ein Gerät eine IP-Adresse und eine Subnetzmaske 71
- DHCP-Adressierung 71
- Statische Adressierung 71
- Auto-IP-Adressierung 71

13. Technische Daten 72
- Schnittstellen/standard 72
- WAN-Schnittstelle 72
- LAN-Schnittstelle 72
- Wireless-LAN-Schnittstelle 72
- Sprachschnittstelle 72
- DSL(ATM)-Eigenschaften 72
- Routing/Bridging 73
- NAT 73
- QoS 73
- Fernwartung 73
- Sicherheit 74
- Umgebungsspezifikationen 74
- Stromadapter 74
- Konformitätserklärung 75

14. Glossar 77

1 Willkommen

Dieses Handbuch beschreibt, wie das PRG AV4202N installiert und konfiguriert wird und richtet sich an die Personen, die verantwortlich für das Installieren und Einrichten der Netzwerkumgebung sind. Daher werden Grundkenntnisse über LANs (lokale Netzwerke) und Internet-Router vorausgesetzt.

Info

In diesem Handbuch wird das PRG AV4202N als „Wireless Router" bezeichnet.
Mit „Ethernet-Kabel" sind Ethernet-Kabel der Kategorie 5 gemeint.

Bitte beachten Sie, dass nicht alle Einstellungen geändert werden können.

Hinweissymbol

Informationshinweis
Informationen, die wichtige Merkmale oder Anweisungen beschreiben.

Vorsicht
Informationen, die auf einen möglichen Datenverlust oder Schäden an einer Anwendung, einem System oder Gerät hinweisen.

Warnung
Information, die Sie vor einer möglichen Verletzungsgefahr warnt.

Textkonventionen

Die Wörter „eingeben" und „schreiben"
Wenn Sie das Wort „eingeben" in diesem Handbuch sehen, müssen Sie etwas eingeben und dann „Return" oder „Enter" drücken. „Return" oder „Enter" sollte nicht gedrückt werden, wenn eine Anweisung einfach nur lautet „schreiben".

Tastenbezeichnungen
Wenn Sie zwei oder mehrere Tasten gleichzeitig drücken sollen, werden die Tastenbezeichnungen mit einem Plus-Zeichen (+) verbunden. Beispiel: Drücken Sie Ctrl+Alt+Del

2 Einleitung

Einleitung

Das PRG AV4202N wurde als kosteneffiziente Lösung für eine einzige Beitbandinternetverbindung zwischen verkabelten und drahtlosen Computern entwickelt. Der Router bietet bietet zudem auch Schutz in Form einer elektronischen „Firewall", die Personen außerhalb des Netzwerks daran hindert, auf Ihre Dateien zuzugreifen oder Ihre Computer zu beschädigen.

Das PRG AV4202N ist ein VDSL2 Router für Heimumgebungen und kleine Büros bzw. Heimbüros. Es liefert Breitbanddienste von einem einzigen modularen Access Point.

Das PRG AV4202N ist die ideale Lösung, um:

- mehrere PCs und Videospielekonsolen miteinander zu verbinden,
- Breitbandinternetverbindungen mit allen Heimcomputern gemeinsam zu nutzen,
- Drucker und Peripheriegeräte gemeinsam zu nutzen.

Der Router setzt eine sehr hohe Bitrate für eine digitale Anschlussleitung (DSL) (2/2+) im Dauerbetrieb mit der Telefonleitung auf der WAN-Seite sowie verschiedene lokale Verbindungstechnologien auf der LAN-Seite um:

- vier geschaltete 10/100 Base-TX Ethernet-Ports
- zwei USB 2.0 Host Ports für externe USB-Peripheriegeräte
- ein IEEE 802.11b/n Wireless LAN Access Point
- zwei FXS Ports für analoge Telefone

Abbildung 1 zeigt ein Beispielnetzwerk. Die Verbindungen erfolgen direkt über den Router. Dadurch kann die Anzahl der Computer in Ihrem Netzwerk erhöht werden.

Vorteile des Routers

- gemeinsam genutzte Internetverbindung für verkabelte und drahtlose Computer
- drahtlose Vernetzung mit Hochgeschwindigkeit 802.11b/g/n
- kein eigener Computer im Dauerbetrieb erforderlich, der die Internetverbindung bereitstellt
- übergreifender Plattform-Betrieb für die Kompatibilität mit Microsoft® Windows und Apple® MAC Computer (siehe technische Beschreibung für unterstützte Plattformen)
- einfache, webbasierte Installation und Konfiguration
- Zentralisierung aller Einstellungen der Netzwerkadressen (DHCP)
- ein virtueller Server für den Fernzugriff auf Web, FTP und andere Dienste in Ihrem Netzwerk
- Sicherheit – in Form einer Firewall – gegen Angriffe von Internethackern sowie eine Verschlüsselung, um den drahtlosen Netzwerkdatenverkehr zu schützen
- Kommunikationsausweichlösung auf analoge Leitungen bei Strom- oder Hardwareausfällen (wenn dies von Ihrem Netzwerkbetreiber unterstützt wird)
- eine zweisprachige GUI

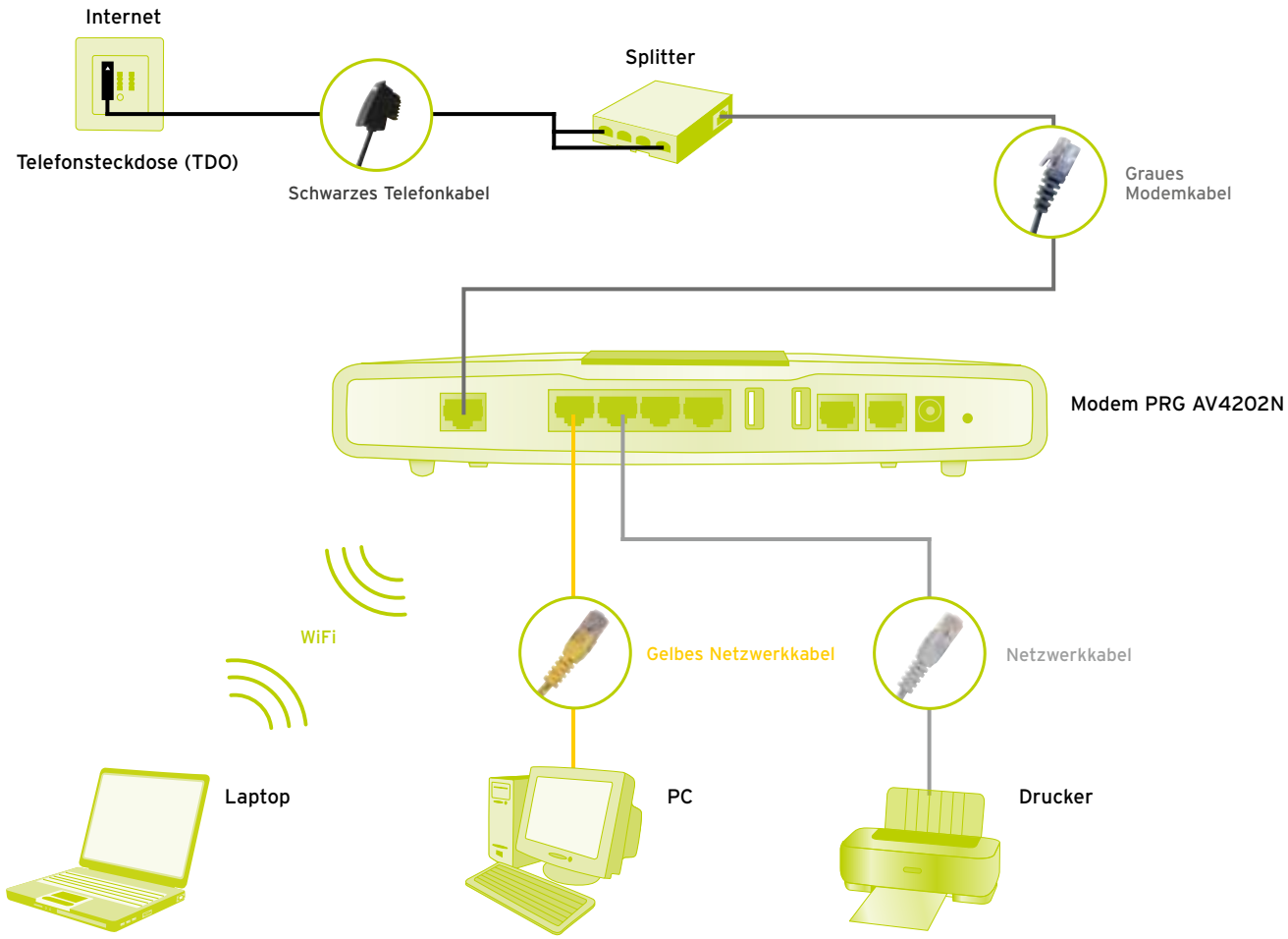
2 Einleitung

Mindestvoraussetzungen für System und Komponenten

Für Ihren Router müssen die Computer und Komponenten in Ihrem Netzwerk folgende Mindestkonfigurationen aufweisen:

- Computer mit Betriebssystemen, die TCP/IP-Netzwerkprotokolle unterstützen, wie Microsoft® Windows 98SE, Windows ME, Windows 2000, Windows XP 32bit, Windows 7 und Vista oder Apple® MAC 10.x
- Eine Netzwerkkarte (NIC) Ethernet 10 Mbits oder 10/100 Mbits pro Computer für den Anschluss an einen der vier Ethernet Ports auf der Rückseite des Routers.
- einen USB-2.0-Anschluss
- optional eine 802.11b/g drahtlose NIC
- mindestens 60 MB freier Festplattenspeicher
- mindestens 128 MB RAM
- unterstützte Browser: Internet Explorer 5.5 oder höher, Firefox 3.0 oder höher

Beispiel für ein Heimnetzwerk



2 Einleitung

Vorderseite

Die Vorderseite des Routers enthält sieben Kontrolllampen (LEDs), die den Status des Netzwerk- und Verbindungsbetriebs anzeigen.

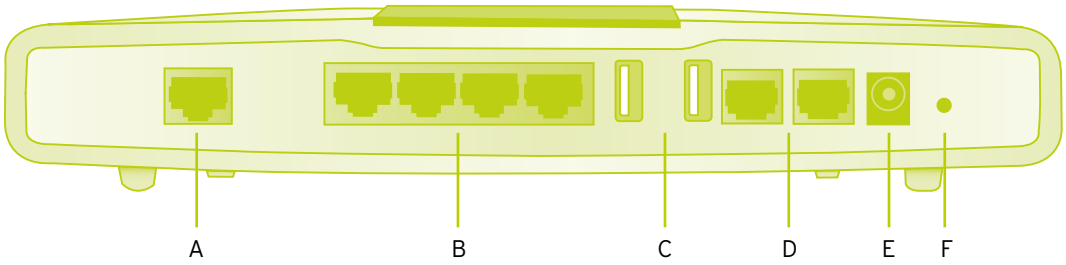
LEDs Vorderseite:

Bez.	LED	LED-Farbe		LED-Beschreibung
1	Strom	Weiß/Rot	Ständiges Weiß	angeschaltet
			Ständiges Rot	Softwarefehler
			Aus	ausgeschaltet
2	Internet-aktivität	Weiß/Rot	Ständiges Weiß	WAN IP-Adresse verfügbar (z. B. PPP aktiv)
			Blinkt Weiß	Eine Verbindung wird aufgebaut.
			Ständiges Rot	DSL ist verbunden, aber es besteht keine Verbindung zum Internet.
3	Telefon		Weiß	Einer der FXS Ports wurde mit einem SIP Proxyserver registriert.
			Blinkt	Eines der am FXS-Port angeschlossenen Telefone ist nicht aufgelegt.
			Rot	Modem nicht registriert
4	Wireless LAN	Blau	An	Wireless-Funktionen aktiviert
			Aus	Wireless-Funktionen deaktiviert

Rückseite

Auf der Rückseite des Routers befinden sich eine „Reset"-Taste, ein Anschluss für das Netzteil, vier LAN-Anschlüsse, ein DSL-Anschluss, zwei USB-Host-Anschlüsse und zwei FXS-Anschlüsse.

Anschlüsse auf der Rückseite:



A Telefon-DSL-Anschluss (2/2+)
B Vier Ethernet Ports 10/100 Mbps
C USB 2.0 Host Port
D FXS Port
E Stromanschluss
F „Reset"-Taste für Zurücksetzung auf Werkseinstellungen

Der Ein- und Ausschalter befindet sich an der Seite des Geräts.

3 Installation der Hardware

Einleitung

Dieses Kapitel führt Sie durch die grundlegende Installation des Routers, einschließlich:

1. Aufstellen des PRG AV4202N
2. Splitter installieren
3. Router mit Ihrem Netzwerk verbinden
4. Ihren Computer für das Netzwerk mit dem Router einrichten

Beachten Sie bitte genau die die Sicherheitshinweise im Anhang „A“.

Aufstellen des Routers

Sie sollten den Router an einem Ort aufstellen, der sicherstellt, dass:

- er sich in der Nähe einer Steckdose und eines Telefonanschlusses befindet
- Wasser oder Feuchtigkeit nicht ins Gehäuse dringen können
- er sich nicht im direkten Sonnenlicht oder in der Nähe von Wärmequellen befindet
- die Kabel nicht in der Nähe von Stromleitungen, Neonröhren und elektrischen Geräten wie Radios, Transmitter und Breitbandverstärkern liegen, die Störungen auslösen könnten.
- er sich möglichst in der Mitte des Netzwerks befindet. Ein geeigneter wäre z. B. auf einem hohen Regal, um die maximale Reichweite für alle verbundenen Geräte sicherzustellen.

3 Installation der Hardware

Router einschalten

Um den Router einzuschalten:

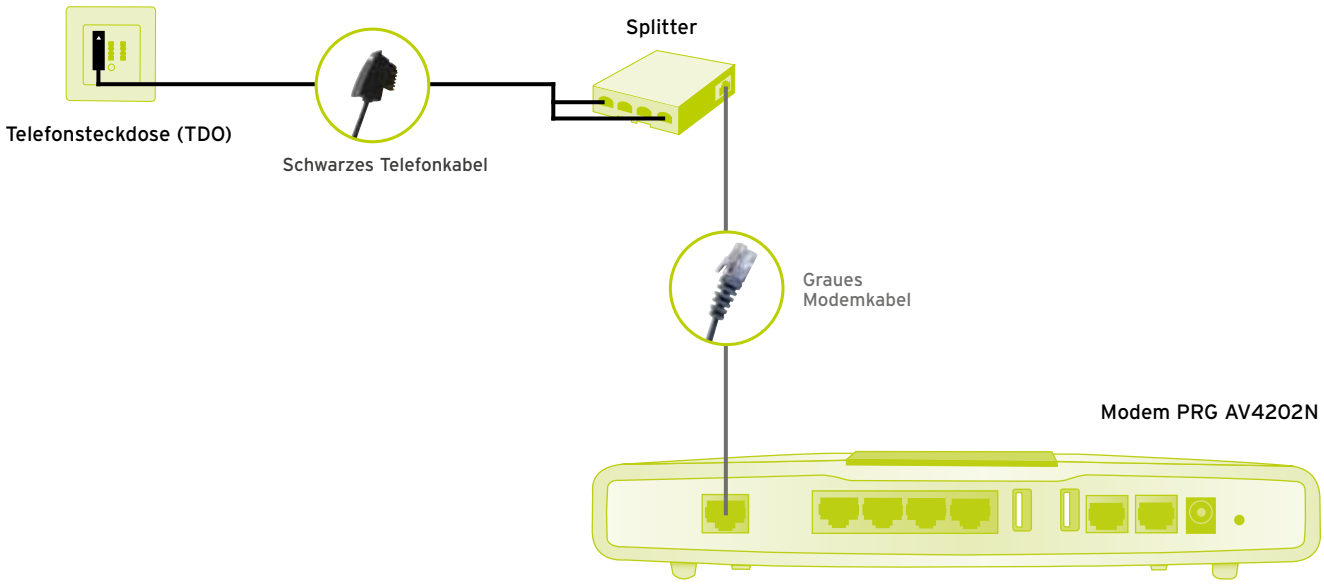
1. Stecken Sie das Netzteil in den Netzteilanschluss auf der Rückseite des Routers.
2. Stecken Sie das Netzteil in eine herkömmliche Wandsteckdose.
3. Drücken Sie den Ein- und Ausschaltknopf auf der Seite des Routers.
4. Warten Sie, bis die LED-Strom-Kontrolllampe ständig weiß leuchtet.

Router verbinden

Der erste Schritt bei der Installation des Routers besteht darin, ihn mit der Telefonsteckdose an der Wand zu verbinden und ihn dann über einen Ethernet- oder USB-Anschluss mit einem Computer zu verbinden.

Telefonkabel anschließen:

1. Stecken Sie ein Ende des Telefonkabels in den DSL-Splitteranschluss, der mit einem Computersymbol gekennzeichnet ist.
2. Stecken Sie das andere Ende des Telefonkabels in den DSL-Anschluss auf der Rückseite des Routers.



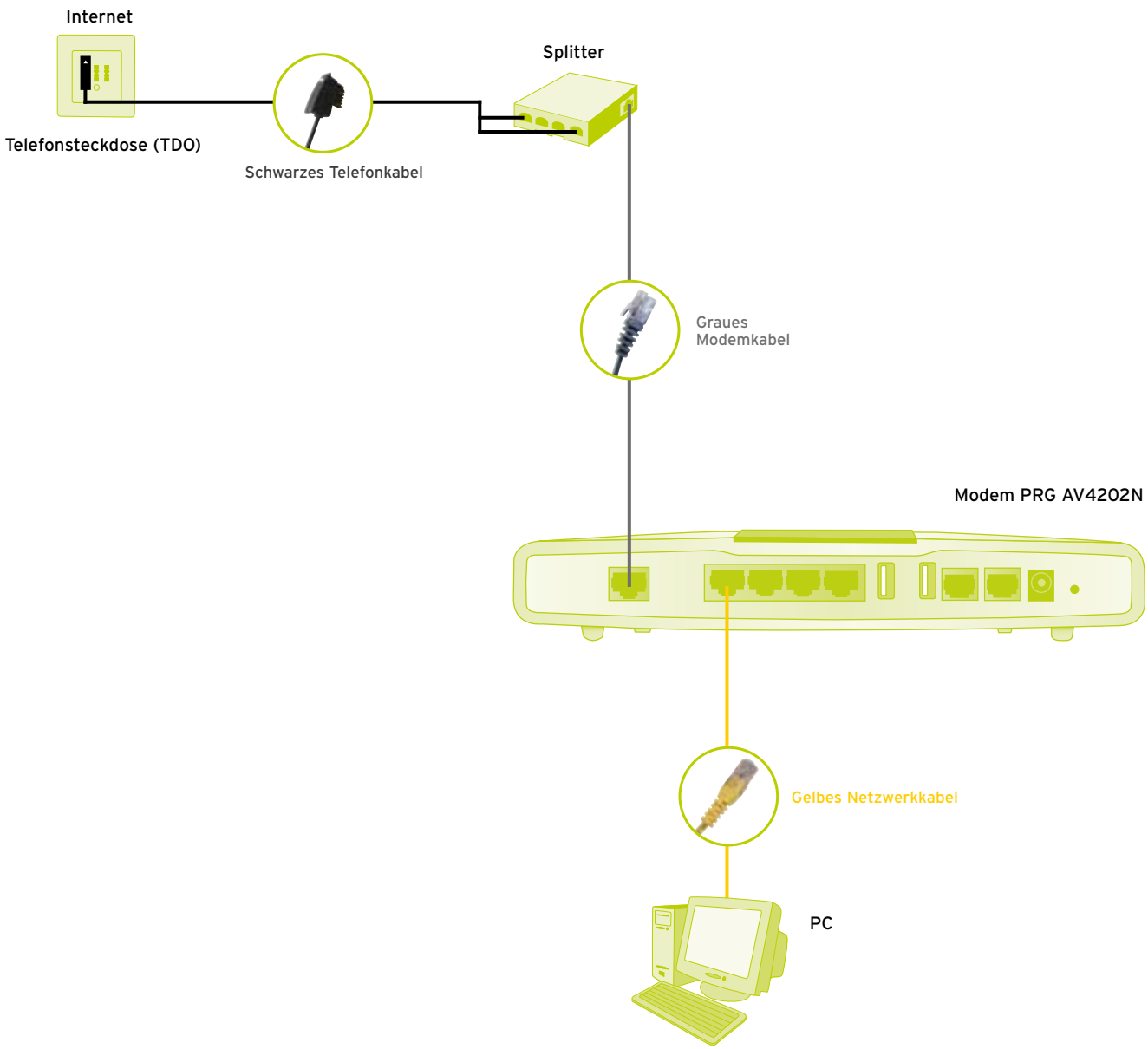
3 Installation der Hardware

Ethernet-Kabel anschließen

1. Stecken Sie ein Ende des Ethernet-Kabels in einen der vier Ethernet-Anschlüsse auf der Rückseite des Routers.

2. Stecken Sie das andere Ende des Ethernet-Kabels in die Ethernet-Netzwerkkarte Ihres Computers.

3. Vergewissern Sie sich, dass die Ethernet-Netzwerkkarte als DHCP Client konfiguriert ist. Wenn dies nicht der Fall ist, konfigurieren Sie sie, damit sie im gleichen lokalen Netzwerk der Routerschnittstelle bleibt (siehe Kapitel „Einrichten Ihres Computers").



4 Installation Ihres Computers

Ethernet-Verbindung

Wenn Sie bereits eine Verbindung mit Ihrem Router eingerichtet haben und/oder Sie manuell eine Verbindung zu Ihrem Router herstellen wollen, folgen Sie bitte den Anweisungen in diesem Kapitel.
Zunächst erfahren Sie, wie eine Ethernet-Verbindung zum Router hergestellt wird. Dazu müssen Sie zuerst prüfen, ob ein TCP/IP-Protokollstapel vorhanden ist, um dann entsprechend Ihrem Betriebssystem eine Ethernet-Verbindung einzurichten. Dazu benötigen Sie eine IP-Adresse für Ihren Computer, die der Router automatisch erstellt. Erst dann fungiert der Router wie der DHCP Server in Ihrem lokalen Netzwerk.

Ethernet-Verbindung: Installation des TCP/IP-Protokolls

Voraussetzung: Auf Ihrem Computer muss das TCP/IP-Protokoll installiert sein. Informationen dazu finden Sie in den folgenden Kapiteln bzw. Handbüchern zu Ihrem Betriebssystem (Microsoft Windows® oder Apple MacOS 10.x).

Microsoft® Windows 98SE, ME, 2000

1. Legen Sie die Windows Installations-CD-ROM in Ihr CD-ROM-Laufwerk ein.
2. Klicken Sie auf „Start“ → „Einstellungen“ → „Steuerung“ → „Netzwerksteuerung“ und doppelklicken Sie „Netzwerk“.
3. Wählenlen Sie „Konfiguration“ → „TCP/IP“ und klicken dann auf „Hinzufügen“
4. Wählen Sie „Protokolle“, klicken auf „Hinzufügen“ und wählen „Microsoft® TCP/IP.“ Klicken Sie dann auf „OK“.
5. Wenn der Computer neu gestartet wird, können Sie die TCP/IP-Einstellungen konfigurieren.
6. Oder weitere Vorgehensweise „siehe Seite 13“.

Microsoft® Windows XP

1. Legen Sie die Windows Installations-CD-ROM in Ihr CD-ROM-Laufwerk ein.
2. Klicken Sie auf „Start“ - „Einstellungen“ - „Steuerung“ und doppelklicken Sie „Netzwerk“.
3. Wählen Sie „Protokoll“ und klicken Sie auf „Hinzufügen“. Wählen Sie „Microsoft® TCP/IP“ und klicken Sie dann auf „OK“.
4. Oder weitere Vorgehensweise „siehe Seite 14“.

Apple® MacOS 10.x

TCP/IP ist auf einem MacOS-System als Teil des Open Transport installiert.

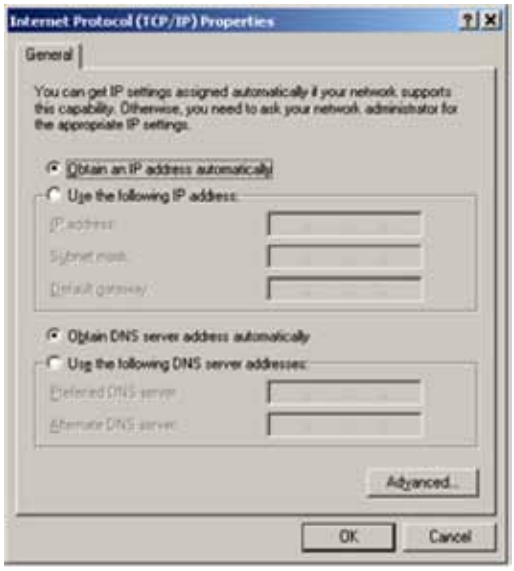
Ethernet-Verbindung: MS Windows 98SE, ME, 2000

TCP/IP konfigurieren Sie auf diesen Betriebssystemen folgendermaßen:

1. Wählen Sie „Start“ ⟶ „Einstellungen“ ⟶ „Steuerung“ und doppelklicken Sie „Netzwerk“.
2. Wählen Sie „Konfiguration“ ⟶ TCP/IP und klicken Sie dann auf „Eigenschaften“.

3. Wenn Sie „IP-Adresse“ anklicken, müssten Sie automatisch eine IP-Adresse erhalten. Klicken Sie auf „OK“.

4. Starten Sie Ihren Computer neu, damit die Änderungen wirksam werden.



5. Geben Sie „http://10.0.0.138/“ in die Adresszeile Ihres Browsers ein, um die Homepage des PRG AV4202N zu öffnen.

Ethernet-Verbindung: MS Windows XP

TCP/IP konfigurieren Sie unter MS Windows XP folgendermaβen:

1.Wählen Sie „Start“ ⟶ „Einstellungen“ ⟶ „Steuerung“ und doppelklicken Sie „Netzwerk“.

2. Wählen Sie „Protokolle“ ⟶ „TCP/IP“ und klicken Sie dann auf „Eigenschaften.“

3. Stellen Sie die Protokolleigenschaften wie in der Abbildung gezeigt ein, um automatisch eine IP-Adresse vom Router zu beziehen. Klicken Sie auf „OK.“

Ethernet-Verbindung: MAC OS 10.x

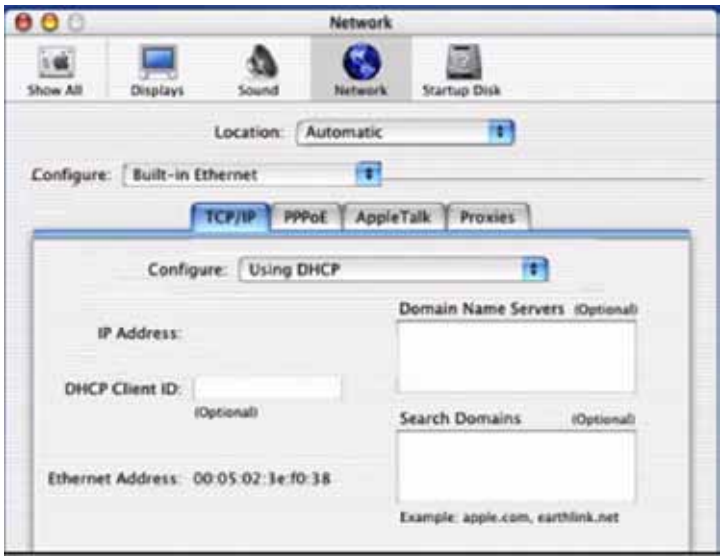
TCP/IP konfigurieren Sie auf MAC OS 10.x folgendermaßen:

1. Öffnen Sie das Apple-Menü → „Systemeinstellungen“ und wählen Sie „Netzwerk“.

2. Wählen Sie aus der Liste „Integriertes Ethernet“. je nach Art der verwendeten Verbindung.

3. Wählen Sie “TCP/IP“.

4. Wählen Sie „DHCP“ aus dem Konfigurationsmenü, um eine dynamische (automatisch generierte) IP-Adresse zu erhalten.



5. Klicken Sie auf „Anwenden“.

6. Klicken Sie auf „Übernehmen“, um die Änderungen zu speichern.

7. Geben Sie „http://10.0.0.138/“ in die Adresszeile Ihres Browsers ein, um die Homepage des PRG AV4202N zu öffnen.

4 Installation Ihres Computers

Wi-Fi - Verbindung

Sie benötigen einen Computer mit 802.11b/g (Wi-Fi-zertifiziert) und installiertem Drahtlosadapter.

1. Installieren Sie den Drahtlosadapter nach den Anweisungen des Herstellers. Nun müsste Ihr Computer eine IP-Adresse zugewiesen bekommen. (DHCP-Modus).

   Sie müssen Ihren Adapter so konfigurieren, dass er mit dem PRG AV4202N den Konfigurationsregeln entsprechend kommuniziert.

2. Im Konfigurationsfenster Ihres Drahtlosadapters finden Sie das Drahtlosnetzwerk (gekennzeichnet mit dem entsprechenden SSID-Namen), das sich in Ihrer Umgebung befindet.

3. Wählen Sie die SSID des PRG AV4202N.

4. Beenden Sie die Konfiguration des Drahtlosadapters mit den gleichen Parametern wie für den PRG AV4202N. Diese sind:

   - RF-Kanal; automatisch suchen (Standard = 6)
   - WPA-Verschlüsseln aktivieren oder deaktivieren (Standard = Deaktivieren)
   - WPA-Schlüsselgröße
   - Verwendeter WPA-Schlüssel

5. Die Funktion der Verbindung können Sie testen, indem Sie „http://10.0.0.138/“ in die Adresszeile Ihres Browsers eingeben und sich mit der Homepage des PRG AV4202N verbinden.

5 Konfiguration des Routers

Einleitung

Das Installationsprogramm des Routers ist webbasiert. Das bedeutet, dass Sie über Ihren Webbrowser Zugriff haben. Zum Webserver des Routers gelangen Sie folgendermaßen:

1. Starten Sie den Webbrowser.

2. Geben Sie „http://10.0.0.138" in die Adresszeile Ihres Browsers ein.

Der Browser besitzt standardmäßig eine IP-Adresse (10.0.0.138). Wenn Sie diese ändern, merken Sie sich bitte die neue IP-Adresse des Routers, da sonst ein „Zurückstellen auf Werkseinstellungen" vorgenommen werden muss, um wieder auf den Router zugreifen zu können.

Der Zugriff auf die Konfigurationsseiten des DSL-Routers wird über die Benutzerkonten gesteuert. Standardmäßig besitzt der User „Admin" uneingeschränkten Zugang, um die Konfiguration des DSL-Routers zu ändern und zu verwalten.

Sie werden aufgefordert, die Sprache der Router-Benutzeroberfläche zu wählen: Englisch oder Deutsch. Danach werden Sie gebeten, einen Benutzernamen und ein Passwort einzugeben (Ausnahme: Für den User „Admin" ist kein Passwort erforderlich).

Auf der linken Seite der Homepage finden Sie ein Menü, das auf allen Webseiten verfügbar und der Ausgangspunkt für jede Konfiguration des Routers. Das vollständige Menü offeriert folgende Optionen:

1. „Home": zeigt eine grafische Darstellung Ihres Netzwerks.

2. „Übersicht": zeigt die Netzwerkübersicht von angeschlossenen oder konfigurierten Geräten.

3. „Schnellinstallation": zur raschen Installation der Router-Verbindung.

4. „Netzwerkverbindungen": zeigt den Status der Netzwerkverbindungen und ermöglicht es, sie zu ändern bzw. neue zu erstellen.

5. „Sicherheit": ermöglicht die Festlegung der Sicherheitsparameter.

6. „Kindersicherung": ermöglicht die Einrichtung der Kindersicherungsfilter.

7. „Erweitert“: ermöglicht den Zugriff auf die erweiterten Konfigurationsseiten und das Festlegen von Router-Parametern für den Nutzerzugriff, die Anmeldungsverwaltung, die Terminierungsregeln, die Sicherung der Router-Konfiguration, etc.

8. „Systemüberwachung“: ermöglicht Diagnosen zur Behebung von Problemen, verwaltet das System und gewährt Zugriff auf Daten verbundener Geräte und Statistiken.

9. „Logout“: Hier melden Sie sich aus der Router-Sitzung ab.

Damit die Änderungen der meisten Geräteparameter wirksam werden, müssen Sie auf „Anwenden“ klicken, um die Änderungen dauerhaft zu speichern. In einigen Fällen ist ein Neustart erforderlich.

5 Konfiguration des Routers

Verfügbare Netzwerkoptionen

Internet.

DSL-Fernnetz- (WAN)-Verbindung. Ermöglicht die WAN-Schnittstelle zu konfigurieren.

Ethernet-Fernnetz (WAN)- oder eine Ethernet-Lokalnetz (LAN)- Verbindung. Ermöglicht, die WAN-Schnittstelle oder das Ethernet-LAN-Gerät zu konfigurieren.

Firewall des Gateways. Die Höhe der Mauer entspricht der aktuell gewählten Sicherheitsebene: „Minimum", „Standard" oder „Maximum". Ermöglicht, die Sicherheitseinstellungen zu konfigurieren.

USB-LAN-Verbindung. Ermöglicht, die Netzwerkparameter für das USB-LAN-Gerät zu konfigurieren.

Wireless-LAN-Verbindung. Ermöglicht, die Netzwerkparameter für das Wireless-LAN-Gerät zu konfigurieren.

Bridge, die mit dem Heimnetzwerk verbunden ist. Zeigt die durch die Bridge verbundenen Geräte.

Computer (Host), der mit dem Heimnetzwerk verbunden ist. Jeder mit dem Netzwerk verbundene Computer erscheint unter dem Symbol der Verbindung, mit der er mit dem Router verbunden ist. Ermöglicht, die Netzwerk-Informationen für den entsprechenden Computer abzurufen.

Drucker, der mit dem Router verbunden ist und von den Netzwerknutzern gemeinsam verwendet wird. Ermöglicht, die Drucker-Einstellungen abzurufen.

File Server, der mit Router verbunden ist und von den Netzwerknutzern gemeinsam verwendet wird. Ermöglicht, die Konfiguration des File Servers angezeigt zu bekommen.

6 Netzwerkverbindungen

Der Zugang zur Administration der Netzwerkverbindungen erfolgt von der Startseite der Homepage des PRG AV4202N.

Beachten Sie bitte, dass eine Änderung der Konfiguration Ihre Konnektivität beeinträchtigen kann.

Unter „Netzwerkverbindungen“ finden Sie eine Übersicht über die Verbindungen des Routers wie WAN- und LAN-Schnittstellen (d.h. Ethernet, USB und drahtlose). Das PRG AV4202N unterstützt sowohl physikalische als auch logische Netzwerkverbindungen. Auf der Bildschirmseite „Netzwerkverbindungen“ können Sie die verschiedenen Parameter Ihrer physikalischen Verbindungen, das LAN und WAN konfigurieren und neue Verbindungen erstellen, indem Sie Tunneling-Protokolle über bestehende Verbindungen wie PPP und VPN verwenden. Klicken Sie auf „Erweitert“, um den Bildschirm zu erweitern und alle Verbindungseinträge sichtbar zu machen.

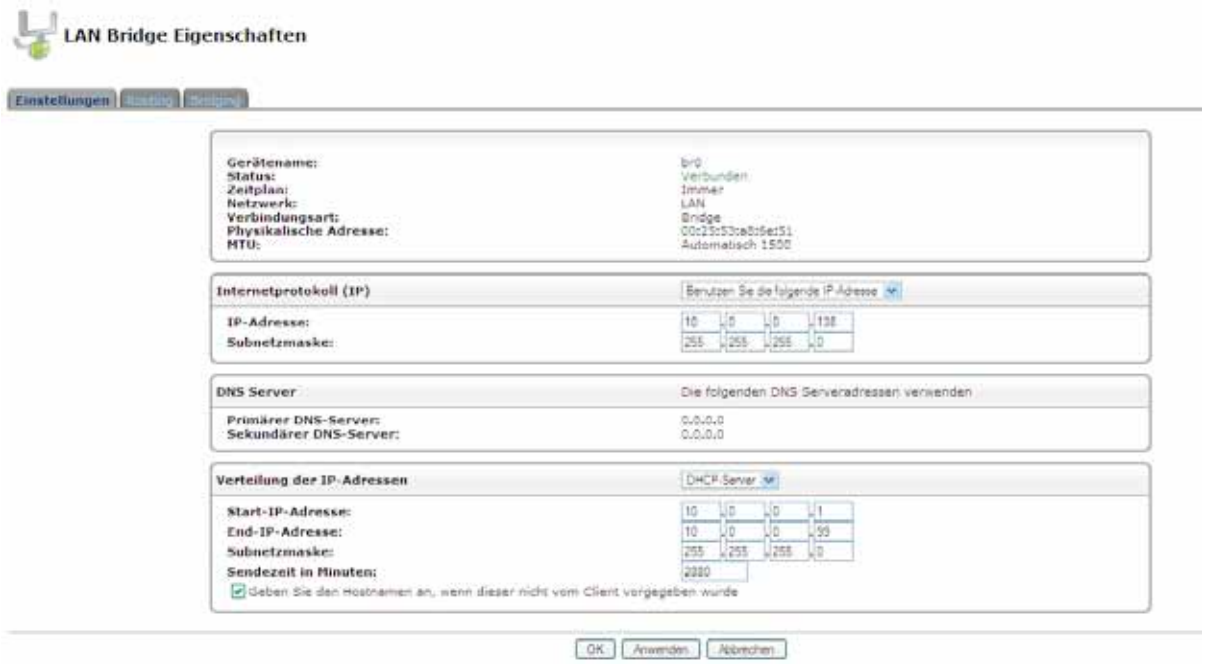
LAN Bridge

Die LAN-Bridge-Verbindung wird verwendet, um mehrere LAN-Geräte in einem virtuellen Netzwerk zu kombinieren, zum Beispiel für das Erstellen eines neuen Netzwerks für LAN-Ethernet und LAN-Drahtlosgeräte. Bitte beachten Sie dass, wenn eine Bridge entfernt wird, die ihr zuvor unterliegenden Geräte die DHCP-Einstellungen der Bridge übernehmen. Zum Beispiel konfiguriert das Entfernen einer Bridge, die als DHCP Client konfiguriert ist, automatisch die LAN-Geräte, die vorher die Bridge als DHCP Clients gebildet haben, mit der genauen DHCP-Client-Konfiguration.

LAN Bridge: Allgemein

Um die Verbindungseinstellungen der LAN Bridge abzurufen und zu bearbeiten, klicken Sie auf den Link „LAN Bridge“ auf der Bildschirmseite „Netzwerkverbindungen“. Die Seite „LAN Bridge Eigenschaften“ scheint auf und zeigt eine detaillierte Übersicht der Verbindungsparameter unter „Allgemein“ an. Diese Parameter können in den übrigen Kategorien der Bildschirmseiten, wie in den folgenden Abschnitten beschrieben, bearbeitet werden.

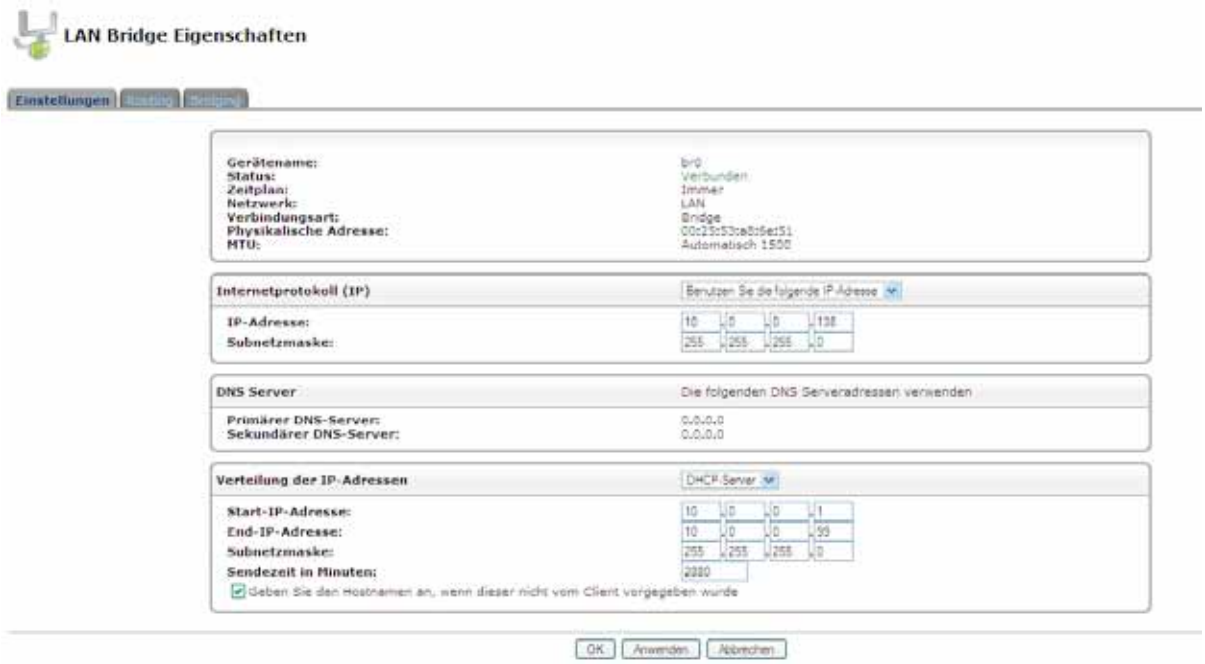
6 Netzwerkverbindungen



LAN Bridge: Einstellungen

Dieser Abschnitt zeigt die allgemeinen Verbindungsparameter an. Es wird empfohlen, die Standardeinstellungen nicht zu ändern, wenn Sie mit den Netzwerkkonzepten nicht vertraut sind, die sie zeigen. Da Ihr Gateway so konfiguriert ist, dass es mit den Standardeinstellungen arbeitet, sind keine Parameter-Änderungen erforderlich.

6 Netzwerkverbindungen



Schedule (Terminierung). Standardmäßig ist die Verbindung immer aktiv. Sie können jedoch Terminierungsregeln konfigurieren, um Zeitabschnitte festzulegen, in denen die Verbindung aktiv sein soll. Wenn eine oder mehrere Terminierungsregel(n) festgelegt wurde(n), verändert sich dieses Feld zu einer Combobox und ermöglicht die Wahl zwischen den verfügbaren Terminierungsregeln.

Network (Netzwerk). Bestimmen Sie, ob sich die Parameter, die Sie konfigurieren, auf eine WAN-, LAN- oder DMZ-Verbindung beziehen, indem Sie die zutreffende Verbindungsart in der Combobox auswählen.

Physical Address (Physikalische Adresse). Die physikalische Adresse Ihrer Netzwerkkarte, die für Ihr Netzwerk verwendet wird. Einige Karten ermöglichen es, diese Adresse zu ändern.

MTU. (Maximum Transmission Unit). Bezeichnet die größtmögliche Paketgröße, die für Internetübertragungen zugelassen ist. In der Standardeinstellung „automatisch" wählt das Gateway die für Ihre Internetverbindung am besten geeignete MTU. Wenn Sie die Funktion „Automatisch durch DHCP" aktivieren, bestimmt der DHCP die MTU. In der Funktion „Manuell" wird empfohlen, einen Wert im Bereich 1200 bis 1500 einzugeben.

Internet Protocol (Internetprotokoll). Wählen Sie eine der folgenden Internetprotokolloptionen aus der Combobox „Internetprotokol!“:

- „Keine IP-Adresse“: Wählen Sie „Keine IP-Adresse“, wenn Ihr Gateway keine IP-Adresse haben soll. Dies kann sinnvoll sein, wenn Sie in einer Umgebung arbeiten, wo Sie mit keinen anderen Netzwerken, wie zum Beispiel dem Internet, verbunden sind.

- „Eine IP-Adresse automatisch beziehen“: Ihre Verbindung ist standardmäßig so konfiguriert, dass sie als DHCP Client agiert. Sie sollten diese Konfiguration beibehalten, falls Ihr Dienstanbieter DHCP unterstützt oder wenn Sie sich mit einer dynamischen IP-Adresse verbinden. Der Server, der dem Gateway eine IP-Adresse zuweist, weist auch eine Subnetzmaske zu. Sie können die dynamisch zugewiesene Subnetzmaske aufheben, indem Sie „Subnetzmaske aufheben“ wählen und stattdessen Ihre eigene Maske angeben. Drücken Sie auf „Freigeben“, um die aktuelle IP-Adresse freizugeben. Wenn die IP-Adresse freigegeben wurde, ändert sich der Text der Schaltfläche in ‚Erneuern‘. Klicken Sie auf „Erneuern“ um die IP-Adresse zu erneuern.

- „Verwenden Sie die folgende IP-Adresse“: Ihre Verbindung kann mit einer permanenten (statischen) IP-Adresse konfiguriert werden. Ihr Dienstanbieter sollte eine solche IP-Adresse und Subnetzmaske zur Verfügung stellen.

DNS Server. Mit dem Domain Name System (DNS) können Webseiten-Domainnamen in IP-Adressen umgewandelt werden. Sie können die Verbindung konfigurieren, um automatisch eine DNS-Serveradresse zu erhalten oder eine Adresse manuell anzugeben, je nachdem welche Angaben Ihr ISP zur Verfügung stellt. Wenn Sie zuvor “Eine IP-Adresse automatisch beziehen” gewählt haben, erscheint eine Combobox. Um die Verbindung so zu konfigurieren, dass sie automatisch eine DNS-Serveradresse bezieht, wählen Sie „DNS Serveradresse automatisch beziehen“ aus dem „DNS Server“ Dropdown-Menü.

IP Address Distribution (IP-Adresszuweisung). Der Abschnitt „IP-Adresszuweisung“ ermöglicht Ihnen, die Server-parameter des Dynamic Host Configuration Protokolls (DHCP) des Gateways zu konfigurieren. Das DHCP weist den Netzwerkcomputern automatisch IP-Adressen zu. Wenn Sie diese Funktion aktivieren, stellen Sie sicher, dass Sie auch Ihre Netzwerkcomputer als DHCP Clients konfigurieren. Wählen Sie eine der folgenden Optionen aus der Combobox „IP-Adresszuweisung“:

DHCP Server.

Start-IP-Adresse: Die erste IP-Adresse, die einem LAN-Host zugewiesen wird. Da die Standard-IP-Adresse des Gateways 10.0.0.138 ist, muss diese Adresse im Bereich zwischen 10.0.0.1 und 10.0.0.99 liegen.

End-IP-Adresse: Die letzte IP-Adresse in dem Bereich, die verwendet werden kann, um LAN-Hosts automatisch IP-Adressen zuzuweisen.

Subnetzmaske: Eine Maske, die verwendet wird, um zu bestimmen, zu welchem Subnetz eine IP-Adresse gehört. Ein Beispiel für den Wert einer Subnetzmaske ist 255.255.255.0.

Lease-Time In Minuten: Jedes Gerät bekommt eine IP-Adresse vom DHCP Server für die Zeit zugewiesen, in der es sich mit dem Netzwerk verbindet. Wenn diese Zeit abgelaufen ist, ermittelt der Server, ob sich der Computer vom Netzwerk getrennt hat. Wenn ja, kann der Server diese IP-Adresse einem neu verbundenen Computer zuweisen. Diese Funktion stellt sicher, dass nicht verwendete IP-Adressen anderen Computern im Netzwerk zur Verfügung stehen.

Host Name bereitstellen, wenn nicht vom Client angegeben: Wenn der DHCP Client keinen Hostnamen hat, weist ihm das Gateway automatisch einen zu.

DHCP Relais. Ihr Gateway kann als DHCP Relais agieren, wenn Sie sich IP-Adressen von einem anderen DHCP Server als Ihrem Gateway DHCP Server zuweisen lassen möchten. Beachten Sie, dass Sie bei der Wahl dieser Funktion auch das WAN des Routers ändern müssen, damit dieser im Routing-Modus arbeitet.

1. Nachdem Sie „DHCP Relais" aus dem Dropdown-Menü gewählt haben, erscheint der Link „Neue IP-Adresse": Klicken Sie auf „Neue IP-Adresse". Die Seite „DHCP Relais Serveradresse" öffnet sich.

2. Geben Sie die IP-Adresse des DHCP Servers an.

3. Klicken Sie auf „OK", um die Einstellungen zu speichern. Wählen Sie „Deaktiviert" aus der Combobox, wenn Sie Ihren Netzwerkcomputern statische IP-Adressen zuweisen wollen.

LAN Bridge: Routing

Sie können für Ihr Gateway entweder statisches oder dynamisches Routing wählen. Das dynamische Routing entscheidet automatisch, wie Datenpakete im Netzwerk übertragen werden. Das statische Routing bestimmt einen festen Routing-Pfad zu benachbarten Zielorten.

Routing Mode (Routing Modus). Wählen Sie einen der folgenden Routing-Modi:

- Route: Wählen Sie den Route-Modus, wenn Sie wollen, dass Ihr Gateway als Router zwischen zwei Netzwerken funktioniert.
- NAPT: Network Address and Port Translation (NAPT) bezieht sich auf die Netzwerkadressübersetzung, einschließlich der Abbildung von Port-Nummern, die es ermöglicht, dass mehrere Geräte eine einzige IP-Adresse gemeinsam nutzen. Verwenden Sie NAPT, wenn Ihr LAN mehrere Geräte umfasst - eine Topologie, welche die Portübersetzung zusätzlich zur Adressübersetzung erfordert.

Device Metric (Geräte-Metric). Der Geräte-Metric ist ein Wert, der vom Gateway verwendet wird, um zu bestimmen, ob eine Route besser ist als eine andere, mit Berücksichtigung von Parametern wie Bandbreite, Verzögerungen und mehr.

Default Route (Standardroute). Aktivieren Sie dieses Feld, um das Gerät als Standardroute festzulegen.

Multicast - IGMP Proxy Internal. IGMP Proxy ermöglicht dem System, IGMP-Host-Nachrichten im Namen von Hosts, die das System durch die Standard-IGMP-Schnittstellen ermittelt hat, auszugeben. IGMP Proxy ermöglicht das Routing von Multicast-Paketen entsprechend den IGMP-Anfragen der LAN-Geräte, die Multicast-Gruppen beitreten wollen. Wählen Sie „Multicast IGMP Proxy Intern", um diese Funktion zu aktivieren.

IGMP Query Version (IGMP-Abfrage-Version). Wenn „Multicast – IGMP Proxy Intern" aktiviert ist, können Sie aus dieser Liste eine Version der unterstützten IGMP auswählen.

Routing Information Protokoll (RIP). Markieren Sie dieses Feld, um das Routing Information Protokoll (RIP) zu aktivieren. RIP bestimmt eine Route, die auf dem kleinsten Hop-Count-Wert zwischen Herkunft und Ziel basiert. Wenn RIP aktiviert ist, wählen Sie Folgendes:

- RIP-Nachrichten anhören – wählen Sie „Keine", „RIPv1", „RIPv2" oder „RIPv1/2".
- RIP-Nachrichten senden – wählen Sie „Keine", „RIPv1" ‚RIPv2-broadcast' oder ‚RIPv2-multicast'.

Routing Table (Routing-Tabelle). Ermöglicht Ihnen, Routen hinzuzufügen oder zu ändern, wenn dieses Gerät aktiv ist. Mit „Neue Route" können Sie eine Route hinzufügen oder bestehende Routen bearbeiten.

LAN Bridge: Bridging

Wenn Sie der Netzwerk-Bridge Geräte angliedern möchten, klicken Sie auf das Symbol „Bearbeiten" in der Spalte VLAN, um die Netzwerkverbindungen speziellen virtuellen LANS zuzuordnen.

6 Netzwerkverbindungen

Markieren Sie „STP", um das Spanning Tree Protokoll auf dem Gerät zu aktivieren. Verwenden Sie es, um sicherzugehen, dass es keine Schleifen in Ihrer Netzwerkkonfiguration gibt und wählen Sie diese Einstellung, wenn Ihr Netzwerk aus mehreren Switches oder anderen Bridges besteht als jenen, die vom Gateway erstellt wurden.

LAN Ethernet

Eine LAN-Ethernet-Verbindung verbindet mehrere Computer über Ethernet-Kabel mit dem Router.

LAN Ethernet: Allgemein

Um die Einstellungen für die LAN-Ethernet-Verbindung aufzurufen und zu bearbeiten, klicken Sie auf den Link „LAN Ethernet" auf der Seite „Netzwerkverbindungen". Die Seite „LAN Ethernet Eigenschaften" erscheint und zeigt unter „Allgemein" eine detaillierte Übersicht über die Verbindungsparameter. Diese Parameter können in den übrigen Kategorien der Seite bearbeitet werden, wie in den folgenden Abschnitten beschrieben.

6 Netzwerkverbindungen

LAN Ethernet: Einstellungen

Dieser Bereich zeigt die allgemeinen Verbindungsparameter. Es wird empfohlen, die Standardwerte nicht zu ändern, wenn Sie mit den Netzwerkkonzepten, die sie darstellen, nicht vertraut sind. Da Ihr Gateway so konfiguriert ist, dass es mit den Standardwerten arbeitet, sind keine Änderungen der Parameter erforderlich.

LAN Ethernet: Erweitert

Internet Connection Firewall (Internetverbindung Firewall). Die Firewall Ihres Gateways schützt Ihren Computer vor nicht authentifizierten Nutzern, die versuchen, über ein Netzwerk wie das Internet Zugriff auf Ihr Netzwerk zu bekommen. Die Firewall kann pro Netzwerkverbindung aktiviert werden. Um die Firewall in dieser Netzwerkverbindung zu aktivieren, markieren Sie „Aktiviert".

LAN Wireless 802.11n Access Point

Das PRG AV4202N integriert verschiedene Schichten drahtloser Sicherheit. Diese beinhaltet das IEEE 802.1x portbasierte Authentifizierungsprotokoll, RADIUS Client, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Wi-Fi geschützter Zugriff (WPA), WPA2, WPA und WPA2 (gemischter Modus) und in der Industrie führende Discus Firewall und VPN-Anwendungen. Zusätzlich ermöglicht der im Router integrierte Authentifizierungs-Server Nutzern eines Heimbüros, autorisierte drahtlose Nutzer festzulegen, ohne dass ein externer RADIUS-Server erforderlich wäre.

6 Netzwerkverbindungen

LAN Wireless 802.11n Access Point: Allgemein

Um die Einstellungen der LAN-Drahtlosverbindung aufzurufen und zu bearbeiten, klicken Sie auf den Link „LAN Wireless 802.11n Access Point“ auf der Seite „Netzwerkverbindungen“. Die Seite „LAN Wireless 802.11n Access Point Eigenschaften“ erscheint und zeigt eine detaillierte Übersicht über die Verbindungsparameter unter „Allgemein“. Diese Parameter können in den übrigen Kategorien der Seite, wie im Folgenden beschrieben, geändert werden.

LAN Wireless 802.11n Access Point: Einstellungen

Dieser Bereich zeigt die allgemeinen Verbindungsparameter. Es wird empfohlen, die Standardwerte nicht zu ändern, wenn Sie mit den Netzwerkkonzepten, die sie darstellen, nicht vertraut sind. Da Ihr Gateway so konfiguriert ist, dass es mit den Standardwerten arbeitet, sind keine Änderungen der Parameter erforderlich.

LAN Wireless 802.11n Access Point: Wireless (drahtlos)

Wireless Access Point
Hier können Sie die grundlegenden Einstellungen des drahtlosen Access Points festlegen.

SSID. Als SSID (Service Set Identifier) bezeichnet man jenen Netzwerknamen, der von allen Teilnehmern eines drahtlosen Netzwerks gemeinsam genutzt wird. Der SSID ist für alle Teilnehmer im drahtlosen Netzwerk identisch. Groß- und Kleinschreibung muss beachtet werden und der Name darf nicht mehr als 32 Zeichen umfassen (Sie können alle Zeichen der Tastatur verwenden). Vergewissern Sie sich, dass die Einstellung für alle Teilnehmer Ihres drahtlosen Netzwerks gleich ist. Eine Änderung der Standard-SSID (openrg) gewährleistet höhere Sicherheit und ist daher empfehlenswert.

SSID Broadcast. Markieren Sie dieses Feld, um SSID Broadcast zu aktivieren. SSID Broadcast wird verwendet, um den Namen des AP (SSID) vor Clients zu verstecken, die von seiner Existenz nichts wissen sollen.

802.11 Mode (Modus). Wählen Sie den drahtlosen Kommunikationsstandard, der kompatibel mit der Drahtloskarte des PCs ist. Sie können entweder mit 802.11n, 802.11g oder im gemischten Modus arbeiten.

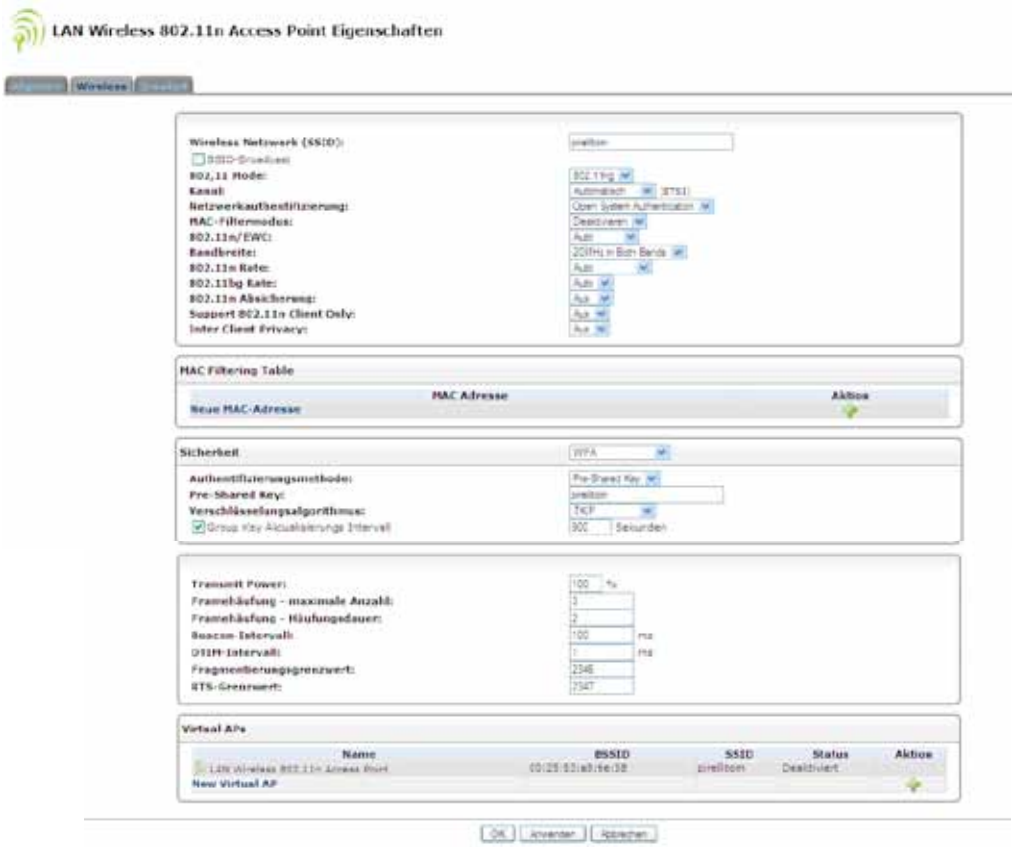
Country (Land). Wählen Sie das zutreffende Land aus der Liste.

Channel (Kanal). Wählen Sie den entsprechenden Kanal aus der Liste, der mit Ihren Netzwerkeinstellungen übereinstimmt. Alle Geräte in Ihrem drahtlosen Netzwerk müssen auf verschiedenen Kanälen liegen, um problemlos zu funktionieren. Die verfügbaren Kanäle hängen von der Regulierungsbehörde ab (in Klammern angegeben), der Ihr Gateway entspricht.

6 Netzwerkverbindungen

Network Authentication (Netzwerk-Authentifizierung). Die WPA-Netzwerk-Authentifizierungsmethode ist eine offene „Systemauthentifizierung". Das bedeutet, dass ein Netzwerkschlüssel nicht für die Authentifizierung verwendet wird. Wenn Sie die Sicherheitsprotokolle 802.1X WEP oder Non-802.1X WEP verwenden, entsteht eine Combobox. Sie bietet die Möglichkeit der „gemeinsam genutzten Schlüssleauthentifizierung" oder kombiniert beide Alternativen.

MAC-Filterungsmodus. Sie können drahtlose Nutzer entsprechend ihrer MAC-Adresse filtern und ihnen entweder den Zugriff erlauben oder verweigern. Dies legen Sie im entsprechenden Dropdown-Menü fest.



MAC Filtering Table (Filterungstabelle)
Hier können Sie erweiterte Einstellungen des drahtlosen Access Points festlegen.

New MAC Address (Neue MAC-Adresse). Klicken Sie auf diesen Link, um die Filterung von MAC-Adressen zu definieren. Geben Sie die zu filternde MAC-Adresse ein und drücken Sie auf "OK". Eine Liste mit MAC-Adressen erscheint, auf welche die gewählte Filterung (erlauben/verweigern) angewendet werden kann.

Security (Sicherheit)
Um die Sicherheitsparameter Ihrer Drahtlosverbindung zu konfigurieren, aktivieren Sie diese Funktion, indem Sie „Aktiviert" markieren. Die Seite aktualisiert sich und zeigt die drahtlosen Sicherheitsoptionen. Wählen Sie aus der Combobox „Stationssicherheitsart" die Art des Sicherheitsprotokolls für das Absichern Ihres drahtlosen Netzwerks. Sie können zwischen WPA, WPA2, 802.1x WEP und Non-802.1x WEP wählen. Die Seite aktualisiert sich und zeigt die für jedes Protokoll entsprechende Konfiguration.

WPA: WPA ist eine Datenverschlüsselungsmethode für 802.11 drahtlose LANs.

Authentification Method (Authentifizierungsmethode). Wählen Sie die Authentifizierungsmethode, die Sie verwenden möchten. Sie können zwischen Pre-Shared Key und 802.1x wählen.

Pre-Shared Key (vorher vereinbarter Schlüssel). Dieser erscheint nur, wenn Sie diese Authentifizierungsmethode gewählt haben. Geben Sie Ihren Verschlüsselungs-Schlüssel ins Feld „Pre-Shared Key" ein. Sie können entweder einen ASCII oder einen Hex-Wert eingeben, indem Sie die Art des Werts in der Combobox wählen.

Encryption Algorithm (Verschlüsselungsalgorithmus). Wählen Sie Temporal Key Integrity Protocol (TKIP) oder Advanced Encryption Standard (AES) als den Verschlüsselungsalgorithmus.

Group Key Update Interval. Legt das Zeitintervall in Sekunden für die Aktualisierung eines Gruppenschlüssels fest.

WPA2: WPA2 ist eine erweiterte Version von WPA und definiert das Protokoll 802.11.

Authentification Method (Authentifizierungsmethode). Wählen Sie die Authentifizierungsmethode, die Sie verwenden möchten. Sie können zwischen Pre-Shared Key und 802.1x wählen.

Pre-Shared Key (vorher vereinbarter Schlüssel). Dieser erscheint nur, wenn Sie diese Authentifizierungsmethode gewählt haben. Geben Sie Ihren Verschlüsselungs-Schlüssel ins Feld „Pre-Shared Key" ein. Sie können entweder einen ASCII oder einen Hex-Wert eingeben, indem Sie die Art des Werts in der Combobox wählen.

Encryption Algorithm (Verschlüsselungsalgorithmus). Der Verschlüsselungsalgorithmus, der für WPA2 verwendet wird, ist Advanced Encryption Standard (AES).

Group Key Update Interval. Legt das Zeitintervall in Sekunden für die Aktualisierung eines Gruppenschlüssels fest.

WPA and WPA2 Mixed Mode (WPA und WPA2 Gemischter Modus):
WPA und WPA2 ist eine gemischte Datenverschlüsselungsmethode.

Authentification Method (Authentifizierungsmethode). Wählen Sie die Authentifizierungsmethode, die Sie verwenden möchten. Sie können zwischen Pre-Shared Key und 802.1x wählen.

Pre-Shared Key (vorher vereinbarter Schlüssel). Das diesbezügliche Eingabefeld erscheint nur, wenn Sie diese Authentifizierungsmethode gewählt haben. Sie müssen dann Ihren Verschlüsselungs-Schlüssel in das Feld „Pre-Shared Key" eingeben. Sie können entweder einen ASCII- oder Hex-Wert wählen. In der Cobobox legen Sie fest, für welche Variante Sie sich entschieden haben.

Encryption Algorithm (Verschlüsselungsalgorithmus). Der Verschlüsselungsalgorithmus, der für WPA und WPA2 verwendet wird, ist entweder Temporal Key Integrity Protocol (TKIP) oder Advanced Encryption Standard (AES).

Group Key Update Interval. Legt das Zeitintervall in Sekunden genau für die Aktualisierung eines Gruppenschlüssels fest.

802.1x WEP: 802.1x WEP ist eine Datenverschlüsselungsmethode, die einen statischen oder automatisch definierten Schlüssel für drahtlose Clients verwendet, die 802.1x für die Authentifizierung und WEP für die Verschlüsselung verwenden. Sie können bis zu vier Schlüssel definieren, aber nur einen gleichzeitig benutzen.

Generate Keys Automatically (Schlüssel automatisch erzeugen). Wählen Sie diese Option, um Verschlüsselungs-Schlüssel automatisch zu erzeugen, anstatt sie manuell einzugeben. Wenn sich die Seite aktualisiert, erscheint die Schlüsselauswahloption nicht mehr auf dem Bildschirm.

Group Key Update Interval. Legt das Zeitintervall in Sekunden genau für die Aktualisierung eines Gruppenschlüssels fest. Der Verschlüsselungs-Schlüssel ist bereits per default aktiviert.

Encryption Method (Verschlüsselungs-Schlüssel). Geben Sie den Verschlüsselungs-Schlüssel ein, wobei alle vorgegebenen Zeichenfelder ausgefüllt werden müssen. Der Schlüssel darf nicht kürzer sein als die vorgegebene Anzahl der Eingabezeichen.

Entry Method (Eingabemethode). Bei der Zeicheneingabe für den Schlüssel können sie Hex oder ASCII wählen.

Key Length (Schlüssellänge). Die Schlüssellänge muss entweder 40 oder 104 bits betragen.

Non-802.1x WEP: Non-802.1xWEP ist eine Datenverschlüsselungsmethode, die einen statisch definierten Schlüssel für drahtlose Clients verwendet, die nicht 802.1x für die Authentifizierung und WEP für die Verschlüsselung verwenden. Die Konfiguration dieser Methode ist nahezu identisch mit der oben beschriebenen 802.1x WEP, mit Ausnahme der automatischen Schlüsselerzeugung und der „Group Key Update"-Spezifikation. Informieren Sie sich unter 802.1x WEP, wenn Sie diese Methode konfigurieren. Beachten Sie bitte, dass der statische Schlüssel auch beim drahtlosen Windows-Client festgelegt werden muss.

Wireless QoS (WMM)
Wi-Fi Multimedia (WMM) bietet grundlegende Qualitätsfunktionen (QoS) für IEEE-802.11-Netzwerke. Wenn Ihre Drahtloskarte WMM unterstützt, aktivieren Sie diese Funktion, indem Sie „Aktiviert" markieren. Bei der Aktivierung von WMM liegt die oberste Priorität auf Sprachdatenpaketen und lässt in Richtung der Hintergrundpakete nach, die die niedrigste Priorität erhalten. Zusätzlich können Sie die Zuverlässigkeit des Datenflusses steuern. Standardmäßig steht die „Ack-Richtlinie" für jede Zugriffskategorie auf „Normal". Das bedeutet, dass ein Quittungspaket für jedes empfangene Paket zurückgeschickt wird. Dies bietet eine zuverlässigere Übertragung, erhöht aber den Datendurchsatz, was zu einer Verminderung der Performance führt. Sie können die Quittierung ausschalten, indem Sie „Keine Ack" in der Combobox für jede Zugriffskategorie wählen und so die Ack-Richtlinie ändern. Dies kann für Sprachübertragungen sinnvoll sein, bei denen die Übertragungsgeschwindigkeit wichtig und ein Paketverlust bis zu einem gewissen Grad akzeptabel ist.

Virtual APs (Virtuelle APs)
Je nach der Anzahl, die von Ihrer Drahtloskarte unterstützt wird, können Sie mehrere drahtlose LANs auf dem PRG AV4202N installieren. Jedes drahtlose LAN ist als Access Point definiert. Der Abschnitt „Virtuelle APs" zeigt den physikalischen Access Point des Routers, auf dem virtuelle Verbindungen erstellt werden können. Um eine virtuelle Verbindung zu erstellen, klicken Sie auf den Link „Neuer Virtueller AP".

Die neue Verbindung wird auch zur Liste der Netzwerkverbindungen hinzugefügt und kann wie jede andere Verbindung konfiguriert werden. Sie können den Namen der Verbindung ändern, indem Sie auf das Symbol „Bearbeiten" klicken und den SSID-Wert auf der Seite „LAN Wireless 802.11n Access Point - Virtueller AP konfigurieren" anklicken.

Wireless WDS
Aktiviert drahtloses Bridging von Access Points innerhalb der Reichweite des Routers. Mit virtuellen Access Points können Sie mit Mitgliedern des WDS-Routers interagieren und so LAN-Nutzern den Zugriff auf entfernte drahtlose Netzwerke gewähren. Ist Wireless WDS aktiviert, wird eine WDS-Liste angezeigt.

LAN Wireless 802.11n Access Point: Erweitert

Internet Connection Firewall (Internetverbindung Firewall). Die Firewall Ihres Gateways schützt Ihren Computer vor nicht authentifizierten Nutzern, die versuchen, über ein Netzwerk wie das Internet Zugriff auf Ihr Netzwerk zu nehmen. Die Firewall kann pro Netzwerkverbindung aktiviert werden. Um die Firewall in dieser Netzwerkverbindung zu aktivieren, markieren Sie „Aktiviert".

Additional IP Addresses (Zusätzliche IP-Adressen). Sie können Alias-Namen (zusätzliche IP-Adressen) zum Gateway hinzufügen, indem Sie auf den Link „Neue IP-Adresse" klicken. Diese Aliase ermöglichen es Ihnen, zusätzlich zu 10.0.0.138 Zugriff auf das Gateway zu nehmen.

6 Netzwerkverbindungen

WAN DSL PPPoE und PPPoA bei ADSL

Die Funktion „WAN DSL“ ermöglicht Ihnen, die WAN-DSL-Leitungsschnittstelle zu überprüfen und zu konfigurieren. Sie können den Login-Namen durch Ihre 10-stellige Kundennummer ersetzen. Das Password finden Sie in Ihrem Datenbrief.

Bitte geben Sie hier Ihren 10-stelligen Login-Namen ein – z. B. 0123456789.

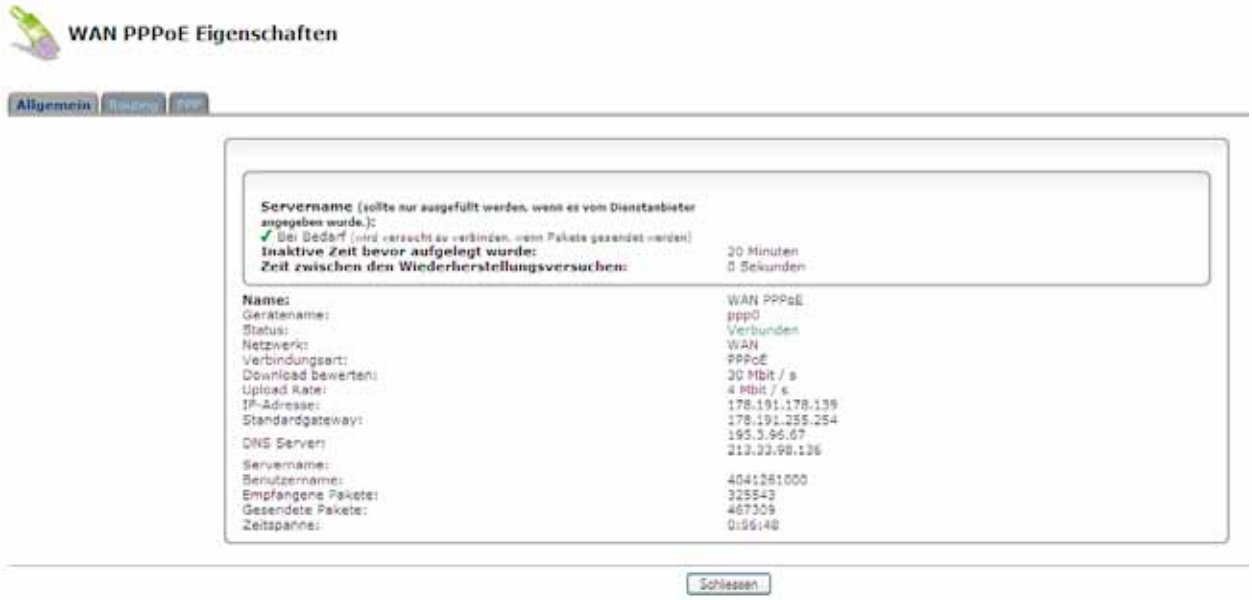
WAN DSL: Allgemein

Mit der Funktion WAN DSL Allgemein können Sie die vordefinierten Einstellungen kontrollieren, aber nicht ändern.

6 Netzwerkverbindungen

WAN DSL: Einstellungen

Unter „WAN-DSL-Einstellungen" können Sie die vorgegebenen Einstellungen kontrollieren.



7 Sicherheit

Dieses Kapitel informiert Sie über die Funktionen im Bereich „Sicherheit", der auf der Homepage des PRG AV4202N verfügbar ist.

Beachten Sie bitte, dass jede Änderung der Konfiguration Ihre Konnektivität beeinträchtigen kann.

Das Gateway-Sicherheitspaket des Routers beinhaltet umfassende und stabile Sicherheitsdienste: Stateful Packet Inspection Firewall, Nutzerauthentifizierungsprotokolle und Passwortschutzmechanismen. All diese Funktionen ermöglichen es den Nutzern, ihre Computer mit dem Internet zu verbinden und gleichzeitig vor Sicherheitslücken im Internet geschützt zu sein.

Die Firewall wurde eigens den Bedürfnissen der Heim- und Büronutzer angepasst und ist vorkonfiguriert, um maximale Sicherheit zu gewährleisten. Die Firewall des Routers liefert jene Sicherheit und Flexibilität, die Heim- und Büronutzer schätzen. Sie bietet ein Höchstmaß an Netzwerksicherheit, und schützt bei interaktiven Anwendungen wie Internetspielen und Videokonferenzen.

Zusätzliche Funktionen wie Webseitenbeschränkungen und Zugangskontrolle können vom Nutzer über die webbasierte Oberfläche oder als Fernzugriff durch den Internetanbieter konfiguriert werden. Die Firewall des Routers unterstützt diese Anwendungen. Sie können spezielle Eingabe- und Ausgaberegeln festlegen, die Reihenfolge logisch ähnlicher Regelpakete bestimmen und zwischen Regeln wählen, die für WAN- und LAN-Netzwerkgeräte angewendet werden können.

Allgemein

Auf der Bildschirmseite „Allgemein" können die grundlegenden Sicherheitseinstellungen des Gateways konfiguriert werden. Die Firewall reguliert den Datenfluss zwischen Heimnetzwerk und Internet. Sowohl eingehende als auch ausgehende Daten werden untersucht und dann entweder akzeptiert (sie dürfen durch den Router gehen) oder abgewiesen (sie dürfen nicht durch den Router gehen) in Übereinstimmung mit einem flexiblen und konfigurierbaren Regelpaket. Diese Regeln sind entwickelt worden, um unerwünschte Eindringlinge fernzuhalten und gleichzeitig den Heimnutzern zu ermöglichen, auf Internetdienste zuzugreifen.

Die Firewall-Regeln legen fest, auf welche Arten von Internetdiensten vom Heimnetzwerk aus zugegriffen werden darf und auf welche Arten von Diensten, die im Heimnetzwerk verfügbar sind, vom Internet aus zugegriffen werden kann. Jede Anfrage, die die Firewall empfängt, ob aus dem Internet oder von einem Computer des Heimnetzwerks, wird mit den Firewall-Regeln überprüft, um festzustellen, ob der Zugriff zugelassen wird. Wenn der Zugriff zugelassen wird, sind auch alle weiteren Zugriffe, die sich auf den ersten beziehen, innerhalb dieser Sitzung ebenfalls erlaubt. Zum Beispiel:
Wenn Sie mit Ihrem Webbrowser eine Webseite im Internet aufrufen, wird eine Anfrage an das Internet für diese Seite gesendet. Wenn die Anfrage den Router erreicht, ermittelt die Firewall Art und Herkunft der Anfrage - in diesem Fall HTTP und ein spezieller PC Ihres Heimnetzwerks. Wenn Sie die Zugangskontrolle nicht so konfiguriert haben, dass alle Anfragen dieser Art von diesem Computer blockiert werden, erlaubt die Firewall der Anfrage, ins Internet weitergeleitet zu werden. Wenn die Webseite vom Webserver zurückgeschickt wird, verbindet die Firewall sie mit dieser Sitzung und erlaubt ihren Durchgang, unabhängig davon, ob der HTTP-Zugriff aus dem Internet ins Heimnetzwerk blockiert oder erlaubt ist.

7 Sicherheit

Sie können eine von drei vordefinierten Sicherheitsebenen für den Router wählen: Minimum, Standard (ist bereits voreingestellt) und Maximum. Die Tabelle zeigt die unterschiedlichen Funktionen des Routers in den drei Ebenen.

Sicherheitsebene	Anfragen aus dem WAN (Einlangende Daten)	Anfragen aus dem LAN (Ausgehende Daten)
Maximum-Sicherheit*	Blockiert: kein Zugriff aufs Heimnetzwerk vom Internet, außer wie in der Port-Weiterleitung, dem DMZ Host und den Fernzugriffsseiten konfiguriert	Eingeschränkt: standardmäßig, nur herkömmliche Dienste wie Surfen und E-Mail erlaubt
Standard-Sicherheit	Blockiert: kein Zugriff aufs Heimnetzwerk vom Internet, außer wie in der Port-Weiterleitung, dem DMZ Host und den Fernzugriffsseiten konfiguriert	Unbeschränkt: alle Dienste zugelassen mit Ausnahme der Konfiguration der Zugangskontrolle
Minimum-Sicherheit	Unbeschränkt: erlaubt vollen Zugriff vom Internet aufs Heimnetzwerk; alle Verbindungen werden zugelassen	Unbeschränkt: alle Dienste zugelassen mit Ausnahme der Konfiguration der Zugangskontrolle

* Bei „Maximum-Sicherheit" können einige Funktionen von aonTV eingeschränkt sein.

7 Sicherheit

Zugriffskontrolle

Möglicherweise möchten Sie den Zugriff auf bestimmte Internetseiten für bestimmte oder alle Computer des Heimnetzwerks blockieren. . Zum Beispiel möchten Sie einem User verbieten, im Internet zu surfen, einem anderen, dass er Dateien über FTP überträgt und dem ganzen Netzwerk, eingehende E-Mails zu empfangen.

Die Zugriffskontrolle definiert Einschränkungen für Zugriffsversuche aus dem Heimnetzwerk ins Internet und kann so den Datenverkehr in beide Richtungen blockieren. Sie kann aber auch bestimmte Dienste zulassen, wenn „Maximum-Sicherheit" konfiguriert ist. Im obigen Beispiel möchten Sie vielleicht User im Heimnetzwerk daran hindern, E-Mails zu empfangen, indem Sie Abrufversuche an POP3-Server im Internet blockieren.

Es gibt zahlreiche Dienste, die Sie blockieren sollten wie zum Beispiel Spiele- und File-Server. Wenn Sie etwa sicher-gehen wollen, dass Ihre Mitarbeiter/innen Ihr Unternehmen nicht durch illegale Downloads markenrechtlich geschützter Dateien schädigen, können Sie diverse einschlägig bekannte P2P- und File-Sharing-Anwendungen sperren.

Dienste erlauben oder einschränken:

1. Wählen Sie „Zugangskontrolle“ auf der Bildschirmseite „Sicherheit.“ Die Seite „Zugangskontrolle'“ öffnet sich.

2. Klicken Sie auf den Link „Neuer Eintrag.“ Die Seite „Zugangskontrollregel hinzufügen“ erscheint.

3. Die Adress-Combobox gibt Ihnen die Möglichkeit, den Computer oder die Computergruppe festzulegen, für die Sie die Zugangskontrollregeln anwenden wollen. Sie können wählen zwischen einem bestimmten Computer in Ihrem LAN oder „Benutzerdefiniert“. Wenn Sie die Option „Benutzerdefiniert“ wählen, öffnet sich die Seite „Netzwerkobjekt bearbeiten“. Mit der Funktion „Netzwerkobjekt erstellen“ können Sie eine Adresse definieren.

4. Mit der Protokoll-Combobox können Sie das Protokoll, das verwendet werden soll, festlegen. Wählen Sie „Alle Dienste anzeigen“, wenn Sie die Liste der verfügbaren Protokolle öffnen wollen. Wählen Sie ein Protokoll oder fügen Sie ein neues hinzu mit der Option „Benutzerdefiniert“. Sie können nun einen neuen Auftrag definieren.

5. Wählen Sie „Eine HTML Seite an den blockierten Client senden“, um die folgende Nachricht beim Client anzeigen zu lassen: “Zugang verweigert – dieser Computer darf nicht im WAN surfen. Bitte kontaktieren Sie Ihren Admin.“ Wenn diese Mitteilung nicht markiert ist, werden die Datenpakete des Clients einfach ignoriert und er/sie bekommt keine Benachrichtigung.

6. Die Terminierungs-Combobox ermöglicht es Ihnen, den Zeitraum festzulegen, für den diese Regel gelten soll. Standardmäßig ist die Regel immer aktiv. Unter „Benutzerdefiniert“ können Sie jedoch Zugangsbeschränkungen konfigurieren.

7. Klicken Sie auf „OK“, um Ihre Änderungen zu speichern. Die Seite „Zugangskontrolle“ zeigt die Regel an, die Sie gerade hinzugefügt haben.

Portweiterleitung

In seiner Standardeinstellung blockiert das PRG AV4202N alle externen Nutzer, die sich mit Ihrem Netzwerk verbinden oder mit ihm kommunizieren wollen.

So ist das System geschützt vor Hackern, die versuchen, in Ihr Netzwerk einzudringen und es zu beschädigen. Sie können aber Ihr Netzwerk für das Internet auf eingeschränkte und gesteuerte Weise öffnen, um mit einigen Anwendungen vom LAN aus arbeiten zu können (zum Beispiel Spiel-, Sprach- und Chatanwendungen) und Servern im Heimnetzwerk den Zugriff aufs Internet zu ermöglichen. Die Funktion „Portweiterleitung“ unterstützt beide Funktionen. Wenn Sie mit der Netzwerkterminologie und den Konzepten vertraut sind, sind Sie sicher schon auf das Thema „Lokale Server“ gestoßen.

Auf der Seite „Portweiterleitung“ können Sie die Anwendungen festlegen, die einen speziellen Umgang durch den Router erfordern.

Sie müssen nur das Anwendungsprotokoll und die lokale IP-Adresse des Computers wählen, der den Dienst nutzt oder zur Verfügung stellt. Bei Bedarf können Sie neue Protokolle, zusätzlich zu den bereits vorhandenen, die vom Router zur Verfügung gestellt werden, hinzufügen.

Zum Beispiel: Wenn Sie eine File-Transfer-Protocol-Anwendung (FTP) auf einem Ihrer PCs verwenden wollen, wählen Sie einfach „FTP“ aus der Liste und geben die lokale IP-Adresse oder den Hostnamen des jeweiligen Computers ein.

Alle FTP-bezogenen Daten, die am Router aus dem Internet ankommen, werden so an den jeweiligen Computer weitergeleitet. Auf ähnliche Weise können Sie Internetnutzern den Zugriff auf Server innerhalb Ihres Heimnetzwerks gewähren, indem Sie jeden Dienst und den PC, der ihn zur Verfügung stellt, definieren. Dies ist sinnvoll, wenn Sie einen Webserver innerhalb Ihres Heimnetzwerks hosten wollen. Wenn ein Internetnutzer seinen / ihren Webbrowser zur externen IP-Adresse des Routers lenkt, leitet das Gateway die eingehende HTTP-Anfrage an Ihren Webserver weiter.

Mit einer externen IP-Adresse (die Haupt-IP-Adresse des Routers) können verschiedene Anwendungen Ihren LAN-Computern zugeordnet werden, allerdings ist jede Anwendungsart auf einen Computer beschränkt. Zum Beispiel können Sie festlegen, dass FTP die Adresse X verwendet, um Computer A zu erreichen und Telnet verwendet auch die Adresse X, um Computer A zu erreichen. Doch der Versuch, das FTP so einzurichten, dass es Adresse X für beide Computer A und B verwendet, schlägt fehl. Der Router bietet hingegen die Möglichkeit, zusätzliche öffentliche IP-Adressen den Portweiterleitungsregeln hinzuzufügen, die Sie zunächst von Ihrem IPS erhalten müssen, um sie in den „NAT IP-Adressenpool“ einzugeben. Dann können Sie das FTP einrichten, dass es Adresse X für Computer A und Adresse Y für Computer B verwendet. Zusätzlich ermöglicht Ihnen die Portweiterleitung, Daten an einen anderen Port umzuleiten, als den, für den er bestimmt war.

Nehmen wir beispielsweise an, Sie haben einen Webserver, der auf Ihrem PC auf Port 8080 läuft und Sie möchten jedem, der auf den Router über HTTP zugreift, Zugang zu diesem Server bieten. Dann gehen Sie folgendermaßen vor:

- Legen Sie eine Portweiterleitungsregel für den HTTP-Dienst fest, mit der IP-Adresse oder dem Hostnamen des PCs.
- Geben Sie 8080 im Feld „An Port weiterleiten“ an.

Jeder eingehende HTTP-Datenverkehr wird nun an den PC weitergeleitet, der den Webserver auf Port 8080 betreibt.

Wenn Sie einen Portweiterleitungsdienst einrichten, müssen Sie sicherstellen, dass der Port nicht bereits von einer anderen Anwendung benutzt wird, die dann ggf. nicht mehr funktioniert. Wenn Sie etwa die SIP-Signalgebung in Voice over IP benutzen, ist der Port, der benutzt wird (5060), der gleiche, der für die Portweiterleitung für LAN-SIP-Agenten vorgesehen ist.

7 Sicherheit

Um einen neuen Portweiterleitungsdienst hinzuzufügen:

1. Wählen Sie „Portweiterleitung“ auf der Seite „Sicherheitsverwaltung“. Die Seite „Portweiterleitung“ öffnet sich.

2. Klicken Sie auf den Link „Neuer Eintrag“. Die Seite „Portweiterleitungsregel“ erscheint.

3. Markieren Sie „Öffentliche IP-Adresse angeben“, wenn Sie diese Regel auf eine bestimmte IP-Adresse anwenden möchten. Die Seite wird aktualisiert.

4. Geben Sie die zusätzliche externe IP-Adresse im Feld „Öffentliche IP-Adresse“ ein.

5. Geben Sie den Hostnamen oder die IP-Adresse des Computers ein, der den Dienst zur Verfügung stellt (der „Server“) im Feld „Lokaler Host“. Beachten Sie, dass, wenn keine zusätzliche IP-Adresse hinzugefügt wurde, nur ein LAN-Computer zugeordnet werden kann, um einen bestimmten Dienst oder eine Anwendung zur Verfügung zu stellen.

6. Die Protokoll-Combobox ermöglicht es Ihnen, das Protokoll, das verwendet werden soll, zu wählen oder festzulegen. Wählen Sie „Alle Dienste anzeigen“ damit sich die Liste der verfügbaren Protokolle öffnet. Wählen Sie ein Protokoll oder fügen Sie mit der Option „Benutzerdefiniert“ ein neues hinzu. So können Sie einen neuen Dienst hinzufügen und als Protokoll festlegen.

7. Standardmäßig leitet der Router Daten an den gleichen Port wie den eingehenden Port weiter. Wenn Sie den Datenverkehr zu einem anderen Port leiten möchten, wählen Sie „Festlegen“. Die Seite aktualisiert sich und ein zusätzliches Feld erscheint, in das Sie die Portnummer eingeben können.

8. Die Terminierungs-Combobox ermöglicht Ihnen, den Zeitraum festzulegen, für den diese Regel gelten soll. Standardmäßig ist die Regel immer aktiv. Unter „Benutzerdefiniert“ können Sie jedoch Terminierungsregeln konfigurieren.

9. Klicken Sie auf „OK“, um Ihre Änderungen zu speichern. Die Seite „Portweiterleitung“ zeigt eine Übersicht der Regeln, die Sie gerade hinzugefügt haben.

7 Sicherheit

DMZ Host

Die Funktion DMZ (Demilitarized) Host Funktion ermöglicht, einen lokalen Computer für das Internet zu öffnen. Markieren Sie einen DMZ Host, wenn:

- Sie einen bestimmten Internetdienst verwenden möchten, wie zum Beispiel ein Onlinespiel oder Videokonferenzprogramm, das sich nicht in der Portweiterleitungsliste befindet und wofür keine Angaben zum Portreichweitenbereich verfügbar sind.
- Sie einen Computer für alle Dienste ohne Einschränkung öffnen möchten möchten und dafür eine geringere Sicherheit akzeptieren.

Ein DMZ Host wird nicht durch die Firewall geschützt und kann daher leicht angegriffen werden. Das Einrichten eines DMZ Host kann auch andere Computer im Heimnetzwerk gefährden. Wenn Sie einen DMZ Host zulassen, müssen Sie das Sicherheitsrisiko berücksichtigen und ihn ggf. vor Attacken schützen.

Eine Anfrage für Zugriff auf einen Dienst im Heimnetzwerk, wie einen Webserver, wird vom Router bearbeitet. Das PRG AV4202N leitet diese Anfrage an den DMZ Host (wenn einer genannt wurde) weiter, wenn der Dienst nicht von einem anderen PC im Heimnetzwerk zur Verfügung gestellt wird (zugewiesen in der Portweiterleitung). In diesem Fall empfängt dieser PC die Anfrage.

Um einen lokalen Host als DMZ Host zu markieren:

1. Wählen Sie „DMZ Host“ auf der Seite „Sicherheitsverwaltung“ Die Seite „DMZ Host“ erscheint.

2. Geben Sie die lokale IP-Adresse des Computers ein, den Sie als DMZ Host definieren möchten.

3. Klicken Sie auf „OK“, um die Einstellungen zu speichern.

7 Sicherheit

Port Triggering

Port Triggering kann für die dynamische Portweiterleitung verwendet werden. Wenn Sie Port-Triggering-Regeln festlegen, können Sie einlangenden Daten erlauben, an einem speziellen LAN-Host anzukommen, indem Sie andere Ports verwenden als die, die für den ausgehenden Datenverkehr verwendet werden. Dies bezeichnet man als Port Triggering, da der ausgehende Datenverkehr bestimmt, zu welchen Ports der eingehende Datenverkehr geleitet wird.

Denken Sie zum Beispiel an einen Spiele-Server, der über UDP-Protokoll auf Port 2222 erreicht wird. Der Spiele-Server antwortet, indem er den Nutzer über UDP auf Port 3333 verbindet, wenn er die Spielesitzung startet. In diesem Fall müssen Sie das Port Triggering verwenden, da dieses Szenario mit den folgenden Standard-einstellungen der Firewall kollidiert:

- Die Firewall blockiert standardmäßig eingehenden Datenverkehr.
- Der Server antwortet auf die Router IP und die Verbindung wird nicht zu Ihrem Host zurückgeschickt, weil sie kein Teil der Sitzung ist.

Um dieses Problem zu lösen, müssen Sie einen Port-Triggering-Eintrag festlegen, der einlangende Datenr auf dem UDP Port 3333 zulässt, wenn ein LAN-Host Datenverkehr zum UDP Port 2222 erzeugt hat.
Dies führt dazu, dass vom Spiele-Server kommende Daten akzeptiert und zum LAN-Host zurückgeschickt werden, der den ausgehenden Datenverkehr zum UDP Port 2222 veranlasste.

Wählen Sie „Port Triggering“ auf der Seite „Sicherheitsverwaltung“. Die Seite „Port Triggering“ öffnet sich.

7 Sicherheit

Webseiten-Einschränkungen

Sie können den Router so konfigurieren, dass er bestimmte Internetseiten so blockiert, dass auf sie nicht von den Computern im Heimnetzwerk zugegriffen werden kann. Außerdem können Einschränkungen auf eine umfassende und automatisch aktualisierte Liste von Seiten festgelegt werden, auf die nicht zugegriffen werden sollte.

Um eine Webseite zu blockieren:

1. Klicken Sie auf „Webseiteneinschränkungen" auf der Seite „Sicherheitsverwaltung".

2. Klicken Sie auf den Link „Neuer Eintrag". Die Seite „Eingeschränkte Webseite" öffnet sich.

3. Geben Sie die Adressen der Webseiten ein (IP-Adresse oder URL), auf die von Ihrem Heimnetzwerk aus nicht zugegriffen werden soll (alle Webseiten innerhalb der Seite werden ebenso blockiert). Wenn die Webseiten-adresse mehrere IP-Adressen besitzt, löst der Router alle zusätzlichen Adressen auf und fügt sie automatisch der Einschränkungstabelle hinzu.

4. Die Combobox „Lokaler Host" gibt Ihnen die Möglichkeit, den Computer oder die Computergruppe zu bestimmten, für die Sie die Webseiteneinschränkungen definieren möchten. Sie können dabei zwischen einem bestimmten Computer in Ihrem LAN oder „Benutzerdefiniert" wählen. Wenn Sie die Option „Benutzerdefiniert" wählen, erscheint die Seite „Netzwerkobjekte bearbeiten". Die Angabe einer Adresse erfolgt über das Erstellen eines „Netzwerkobjekts".

5. Die Terminierungs-Combobox ermöglicht Ihnen, den Zeitraum festzulegen, für den diese Regel gelten soll. Standardmäßig ist die Regel immer aktiv. Unter „Benutzerdefiniert" können Sie jedoch Terminierungsregeln konfigurieren.

6. Klicken Sie auf „OK", um die Einstellungen zu speichern. Sie werden auf die vorherige Seite zurückgeleitet, während der Router versucht, die Seite zu finden. „Auflösen ..." erscheint in der Statusspalte, während die Seite gesucht wird (die URL wird in eine oder mehr IP-Adressen „aufgelöst").

7 Sicherheit

Verbindungen

Die Verbindungsliste zeigt alle Verbindungen, die aktuell auf der Firewall offen sind, sowie verschiedene Details und Statistiken. Mit dieser Liste können Sie unerwünschte Verbindungen schließen, indem Sie auf ihre „Entfernen"-Schaltflächen klicken. Die Basisanzeige beinhaltet den Namen des Protokolls, die verschiedenen Ports, die sie verwendet, und die Richtung des gesicherten Datenverkehrs.

Klicken Sie auf „Erweitert", um eine detaillierte Verbindungsliste anzuzeigen, welche die Time-to-Live-Verbindung, die Anzahl der Kilobytes und empfangene und übertragene Datenpakete, den Gerätetyp und den Routing-Modus beinhaltet.

Verwenden Sie die Combobox „Verbindungen pro Seite", um die Anzahl der Verbindungen, die gleichzeitig angezeigt werden, auszuwählen. Der „Ungefähre max. Verbindungen" -Wert stellt die Menge der zusätzlichen gleichzeitig möglichen Verbindungen dar.

7 Sicherheit

Sicherheitslog

Der Sicherheitslog zeigt eine Liste von Firewall-bezogenen Vorfällen, einschließlich der Versuche, eingehende und ausgehende Verbindungen aufzubauen, Versuche, sich über eine administrative Oberfläche zu authentifizieren (webbasierte Verwaltung oder Telnet Terminal), Firewall-Konfiguration und Systemstart. Um den Sicherheitslog aufzurufen, klicken Sie auf „Sicherheitslog" auf der Seite „Sicherheitsverwaltung". Die Seite „Sicherheitslog" erscheint.

Zeit. Der Zeitpunkt, in dem der Vorfall aufgetreten ist.

Vorfall. Es gibt fünf Arten von Vorfällen:
- Eingehender Datenverkehr: Der Vorfall betrifft einlangenden Datenverkehr.
- Ausgehender Datenverkehr: Der Vorfall betrifft ausgehenden Datenverkehr.
- Firewall-Installation: Konfigurationsnachricht.
- WBM Login: Weist darauf hin, dass sich ein Nutzer bei WBM (webbasierter Verwaltung) angemeldet hat.
- CLI Login: Weist darauf hin, dass sich ein Nutzer bei CLI (über Telnet) angemeldet hat.

Art des Vorfalls. Eine Beschreibung des Vorfalls:
- Blockiert: Das Datenpaket wurde blockiert. Die Nachricht ist rot gefärbt.
- Akzeptiert: Das Datenpaket wurde akzeptiert. Die Nachricht ist grün gefärbt.

Details. Mehr Details über das Datenpaket oder den Vorfall wie Protokoll, IP-Adressen, Port, etc.

8 Erweitert

Dieses Kapitel beschreibt den Bereich „Erweitert“, der über die Homepage des PRG AV4202N verfügbar ist.

Beachten Sie bitte, dass jede Änderung der Konfiguration Ihre Konnektivität beeinträchtigen kann.

Die Seite „Erweitert“ umfasst Betriebs- und Konfigurationsfunktionen. In diesem Screenshot finden Sie eine Auflistung und Beschreibung der einzelnen Symbole:

8 Erweitert

Benutzer

Sie können Nutzer hinzufügen, bearbeiten und löschen. Sie können Nutzer auch in bestimmten Gruppen zusammenfassen. Um zu den Nutzereinstellungen zu gelangen, klicken Sie auf „Nutzer“ auf der Seite „Erweitert“. Die Seite „Nutzer“ öffnet sich. Die Seite listet die Nutzer und Gruppen auf, die im Router definiert wurden. Der „Administrator'' ist ein Standardnutzer, der vom System geliefert wird.

Um einen neuen Nutzer hinzuzufügen, klicken Sie auf „Neuer Nutzer“. Die Seite „Nutzereinstellungen“ öffnet sich.

- Voller Name: Der volle Name des Fernnutzers.
- Benutzername: Der Name, den ein Nutzer verwendet, um aufs Netzwerk zuzugreifen.
- Neues Passwort: Das Nutzerpasswort.
- Neues Passwort wiederholen: Wenn ein neues Passwort zugewiesen wurde, tippen Sie es erneut ein, um seine Richtigkeit zu bestätigen.
- Primäre Gruppe: Diese Auswahl erscheint nur, nachdem ein Nutzer definiert wurde, sodass Sie die primäre Gruppe wählen können, der dieser Nutzer angehören soll.
- Nutzungsrechte: Wählen Sie die Nutzungsrechte des Nutzers in Ihrem Heimnetzwerk.
- Administratorrechte: Vergeben Sie Rechte, um die Systemeinstellungen über die webbasierte Verwaltung oder Telnet fernzusteuern.
- Fernzugriff über SSL-VPN: Gewähren Sie Fernzugriffsrechte für den Router über das SSL-VPN-Protokoll.
- Mail-Server-Zugriff: Nutzungsrechte, um den Mail Server des Routers zu verwenden. Wenn Sie diese Option wählen, müssen Sie das Homeverzeichnis und die Mailbox des Nutzers in den folgenden Bereichen aktivieren.
- Microsoft File und Printer-Sharing-Zugriff: Nutzungsrechte, um Dateien und Drucker nutzen zu können.
- FTP-Server-Zugriff: Nutzungsrechte, um den FTP-Server des Routers nutzen zu können.
- Zugriff auf den Internetdrucker: Nutzungsrechte, um einen Internet-Printing-Protocol(IPP)-Drucker nutzen zu können.
- Fernzugriff über VPN: Fernzugriff zum Router über das VPN-Protokoll.

8 Erweitert

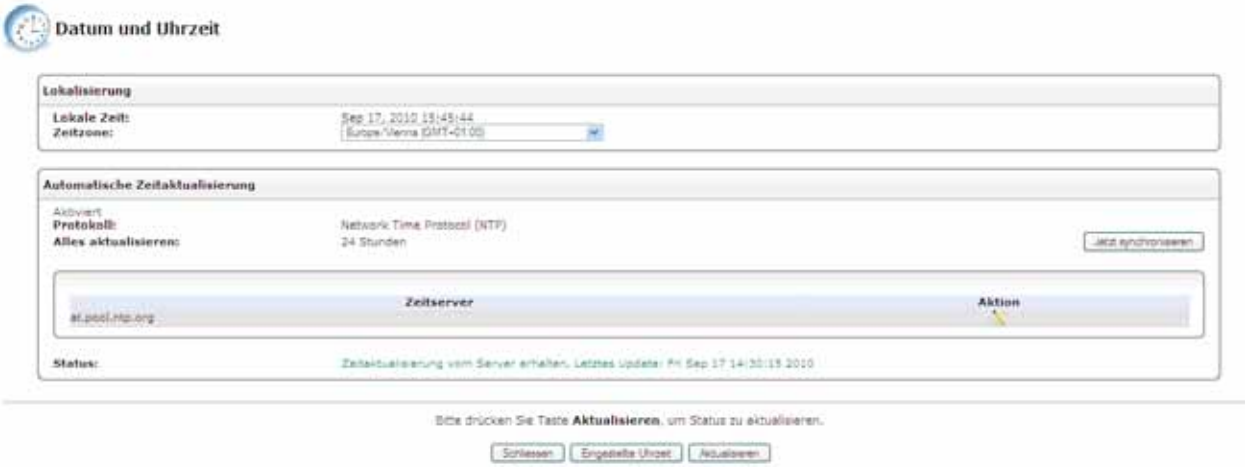
Datum und Uhrzeit

Um das Datum, die Uhrzeit und Winter-/Sommerzeit einzustellen, gehen Sie bitte wie folgt vor:

1. Klicken Sie auf das Symbol „Datum und Uhrzeit“ auf der Seite „Erweitert“ der webbasierten Verwaltung. Die Einstellungen für „Datum & Uhrzeit“ werden angezeigt.

2. Wählen Sie Ihre Zeitzone aus dem Pull-Down-Menü. Der Router kann automatisch die Winter-/Sommerzeit für ausgewählte Zeitzonen einstellen. Wenn die Winter-/Sommerzeit für Ihre Zeitzone nicht automatisch ermittelt wird, werden die folgenden Felder angezeigt:

   - Aktiviert. Markieren Sie die Winter-/Sommerzeit.
   - Start. Datum und Zeit des Beginns der Winter-/Sommerzeit.
   - Ende. Datum und Zeit des Endes der Winter-/Sommerzeit.
   - Aufgehoben. Winter-/Sommerzeit aufgehoben.



8 Erweitert

DDNS

Der Dynamische DNS(DDNS)-Dienst ermöglicht Ihnen, eine dynamische IP-Adresse auf einen statischen Hostnamen zu verweisen. So bleibt Ihr Computer via Internet immer optimal erreichbar. Wenn Sie sich mit dem Internet verbinden, weist Ihnen der Dienstanbieter normalerweise eine nicht genutzte IP-Adresse aus einem Pool von IP-Adressen zu und diese Adresse wird nur für die Dauer einer bestimmten Verbindung genutzt. Die dynamische Adresszuweisung erweitert den nutzbaren Pool der verfügbaren IP-Adressen und hält gleichzeitig einen konstanten Domainnamen aufrecht. Wenn Sie den DDNS-Dienst nutzen, ändert sich jedes Mal, wenn die IP-Adresse, die von Ihrem ISP bereitgestellt wird, die DNS-Datenbank entsprechend, um die Änderung wiederzugeben. So bleibt Ihr Domainname, auch wenn sich Ihre IP-Adresse oft ändern, konstant und erreichbar.

Um die DDNS-Funktion zu nutzen, müssen Sie zunächst ein DDNS-Konto erhalten. Zum Beispiel können Sie auf http://www.dyndns.org/account/create.html ein neues Konto öffnen. Um ein Konto anzuwenden, müssen Sie einen Benutzernamen und ein Passwort angeben.

8 Erweitert

Diagnose

Die Diagnoseseite hilft Ihnen dabei, die Netzwerkkonnektivität zu testen und Statistiken zu kontrollieren, wie zum Beispiel die Anzahl an gesendeten und empfangenen Datenpaketen, die Paketumlaufzeit und den Erfolgsstatus.

Ping (ICMP Echo). Um eine Diagnose der Netzwerkkonnektivität durchzuführen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf das Symbol „Diagnose" auf der Seite „Erweitert" in der webbasierten Verwaltung. Die Seite „Diagnose" öffnet sich.

2. Im Abschnitt Ping (ICMP Echo) geben Sie im Feld „Zielort" die IP-Adresse oder URL ein, die Sie testen möchten.

3. Geben Sie die Anzahl der Pings ein, die Sie durchführen wollen.

4. Drücken Sie auf „Start".

5. Innerhalb weniger Sekunden werden die Diagnosestatistiken angezeigt. Wenn keine neuen Informationen angezeigt werden, drücken Sie auf „Aktualisieren".

ARP. Um einen ARP-Pakettest durchzuführen:
Eine Traceroute durchführen. Um eine Traceroute durchzuführen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf das Symbol „Diagnose" auf der Seite „Erweitert" in der webbasierten Verwaltung. Die Seite „Diagnose" erscheint.

2. Im Bereich Traceroute geben Sie die IP-Adresse oder URL, die Sie testen möchten, im Feld „Zielort" ein.

3. Drücken Sie auf „Start". Eine Traceroute startet, welche die Seite kontinuierlich erneuert.

4. Um die Suche anzuhalten und die Ergebnisse zu kontrollieren, klicken Sie auf „Abbrechen".

8 Erweitert

Disc-Management

Das PRG AV4202N kann als Disc-Manager für externe Speichergeräte fungieren, die über USB oder FireWire verbunden sind. Die LAN-Geräte Ihres Netzwerks können dieses Speichergerät gemeinsam als abgebildetes Netzlaufwerk nutzen und Informationen austauschen, ohne direkt aufeinander zugreifen zu müssen. Die web-basierte Verwaltung ermöglicht Disc-Management-Aufgaben wie Partitionieren und Formatieren.

Eine interne Disc oder ein angeschlossenes Speichergerät erscheint auf der Netzwerkabbildung. Sie können Informationen über die Disk abrufen, indem Sie auf ihr Symbol klicken. Die Seite „Disc-Informationen" erscheint. Für eine umfassende Ansicht klicken Sie auf den Link „Geteilter Speicher" in der Kategorie „Lokales Netzwerk" der webbasierten Verwaltung. Die Seite „Disc-Management" erscheint.

Enabled (Aktiviert). Wählen Sie diese Box an oder ab, um die Funktion zu aktivieren oder deaktivieren.

System Data (Systemdaten). Der Name der Partition, auf der die Systemdaten liegen.

User Data (Nutzerdaten). Der Name der Partition, auf der die Nutzerdaten liegen.

Discs. Dieser Abschnitt zeigt eine Tabelle mit Ihren verbundenen Speichergeräten. Die Spalte „Gerät" zeigt die Namen an, die der Router den verbundenen Geräten gibt. Klicken Sie auf diesen Link, um die „Disc-Informationen" des Geräts anzusehen. Wenn ein Gerät partitioniert ist, zeigt die Spalte „Partitionen" seine Partitionnamen an. Wenn die Partitionen formatiert sind, beinhalten ihre Namen einen Buchstaben.

RAID-Geräte. Dieser Abschnitt zeigt die konfigurierten RAID-Geräte.

8 Erweitert

Druckerserver

Das PRG AV4202N kann als Print-Server agieren. Über diese Seite können die Nutzer die Aufgaben des Print-Servers verwalten und nachverfolgen.

8 Erweitert

File Server

Der Router bietet eine File-Server-Funktion, die es Ihnen ermöglicht, verschiedene Aufgaben in der Dateiverwaltung auszuführen, wie zum Beispiel die Verwaltung von gemeinsam genutzten File Servern und das Festlegen der Zugangskontrollliste. Die File-Server-Funktion ergänzt das Router-Disc-Management. Sie können auf die Einstellungen des File Servers entweder von seinem Link in der Kategorie „Speicher" zugreifen oder indem Sie auf das Symbol „File Server" auf der Seite „Erweitert" klicken. Die Seite „File Server" öffnet sich.

Enabled (Aktiviert). Aktivieren Sie diese Box, um diese Funktion zu nutzen. Auf der Windows Netzwerkabbildung der LAN-Hosts sehen Sie NetBIOS Workgroup bzw. Discus Arbeitsgruppenname.

File Server Shares. Ermöglicht Ihnen, File Shares auf Ihren Disc-Partitionen zu definieren.

FTP-Server

Der Router kann als File Transfer Protocol (FTP) Server agieren und Benutzern und Gästen ermöglichen, auf seine internen Discs zuzugreifen, um einfach (aber sicher) Dateien auszutauschen. Der Router-FTP-Zugang besteht aus zwei Ebenen:

- Benutzerzugang. Registrierte Benutzer können auf vordefinierte Verzeichnisse zugreifen, die durch ihren Benutzernamen und ein Passwort geschützt sind.
- Anonymer Zugriff. Gäste können auf vordefinierte öffentliche Verzeichnisse zugreifen.

8 Erweitert

Konfigurationsdatei

Diese Funktion ermöglicht die gesamte Konfiguration des PRG AV4202N in nur einem Schritt. Sie brauchen nur die Datei zu lokalisieren und den Ladeprozess der Konfigurationsdatei zu starten. Die Konfigurationsdatei ist ein Skript, das alle Parameter enthält, die Sie ändern möchten, und eine Alternative zu den manuellen, schrittweisen Änderungen der gleichen Parameter, die mit Web-Screenshots durchgeführt werden.

Media Sharing

Discus Media Sharing ermöglicht Ihnen, Mediendateien von einem Speichergerät, das mit dem Router verbunden ist, gemeinsam zu nutzen und zu streamen. Sie erreichen die gemeinsam genutzten Mediendateien entweder mit einem netzwerkfähigen Unterhaltungselektronikgerät (CE) oder von einem LAN-PC mit einer installierten Medien-Renderings-Software. In beiden Fällen kommt ein Universal Plug and Play (UPnP) Media-Renderer zum Einsatz.
Die Seite „Media Sharing" enthält folgende Optionen:

Share Music, Pictures and Video on My Local Networks (Musik, Bilder und Videos in meinem lokalen Netzwerk teilen) Diese Option ist standardmäßig aktiviert. Um die Funktion des Media Sharings außer Betrieb zu nehmen, deaktivieren Sie diese Option.

Automatically Share Media in All Folders (Medien automatisch in allen Ordnern gemeinschaftlich nutzen). Standardmäßig ist diese Funktion aktiviert, so dass alle Partitionen und Ordner auf dem Speichergerät automatisch gemeinschaftlich genutzt werden können.

Share Only Recognized Media File Types (Nur bestimmte, definierte Mediendateitypen zur gemeinschaftlichen Nutzung freigeben). Ist diese Funktion aktiviert, können nur bestimmte, definierte Mediendateien gemeinschaftlich genutzt werden.

8 Erweitert

PRG AV4202N Firmware Upgrade (Aktualisierung)

Das PRG AV4202N führt automatische Updates seiner Software durch. Bei diesen Updates bleiben Ihre von Ihnen definierten Konfigurationen und Einstellungen erhalten. Sie können diese Updates auch - als sogenannte Fern-Updates - vom Internet aus initiieren, indem Sie per Fernzugriff eine aktualisierte Software-Imagedatei herunterladen.

Fern-Update

Die Updates versorgen Sie mit der jeweils aktuellen Software-Version und sollten daher routinemäßig bzw. manuell erfolgen. Um die Einstellungen für die automatische Überprüfung und das letzte Überprüfungsergebnis abzurufen, klicken Sie auf das Symbol „Firmware Upgrade" auf der Bildschirmseite „Erweitert". Die Seite „Firmware Aktualisierung" öffnet sich. Im Abschnitt „Aktualisierung vom Internet aus" können Sie die Überprüfungsart und das Zeitintervall für die Updates wählen. Ob eine neue Version verfügbar ist oder nicht, wird nach der letzten durchgeführten Überprüfung in der Zeile zwischen den Schaltflächen „Jetzt überprüfen" und „Upgrade erzwingen" angezeigt.

Wenn eine neue Version verfügbar ist:

→ Drücken Sie auf „Aktualisierung erzwingen". Ein Downloadvorgang startet. Wenn der Download abgeschlossen ist, erscheint ein Bestätigungshinweis, der Sie fragt, ob Sie die neue Version aktivieren wollen.

→ Klicken Sie zur Bestätigung auf „OK". Der Aktualisierungsvorgang startet und sollte nicht länger als eine Minute dauern.

Am Ende des Aktualisierungsvorgangs startet der Router automatisch neu. Die neue Softwareversion wird gestartet. Ihre von Ihnen definierten Konfigurationen und Einstellungen bleiben erhalten. Wenn keine neue Softwareversion verfügbar ist, drücken Sie auf „Jetzt überprüfen", um eine sofortige Überprüfung durchzuführen (anstatt auf die nächste terminierte Überprüfung zu warten). Daraufhin erscheint nun das grüne Insert: „Überprüfung läuft ..."

8 Erweitert

Protokolle

Die Protokollfunktion beinhaltet eine Reihe von voreingestellten und nutzerdefinierten Anwendungen und gemeinsame Porteinstellungen. Sie können Protokolle wie etwa die Zugangskontrolle oder die Portweiterleitung in verschiedenen Sicherheitsfunktionen verwenden. Sie können neue Protokolle hinzufügen oder bestehende bearbeiten.

Um die Basisprotokollliste anzusehen, klicken Sie auf das Symbol „Protokolle" auf der Seite „Erweitert". Drücken Sie auf „Erweitert" unten auf dieser Seite, um die gesamte Liste der vom Router unterstützten Protokolle abzurufen. Um ein Protokoll zu definieren:

1. Klicken Sie auf das Symbol „Protokolle" auf der Seite „Erweitert". Die Seite „Protokolle" erscheint.

2. Klicken Sie auf den Link „Neuer Eintrag", worauf die Seite „Dienst bearbeiten" erscheint.

3. Benennen Sie den Dienst im Feld „Dienstname" und klicken Sie auf den Link „Neue Dienstports". Die Seite „Dienstserverports bearbeiten" erscheint. Sie können jedes der in der Combobox verfügbaren Protokolle wählen oder ein neues hinzufügen, indem Sie „Andere" wählen. Wenn Sie ein Protokoll aus der Combobox wählen, aktualisiert sich die Bildschirmseite und zeigt die entsprechenden Felder, in die Sie die jeweiligen Informationen eingeben können.

4. Wählen Sie ein Protokoll und geben Sie die jeweiligen Informationen ein.

5. Klicken Sie auf „OK", um die Einstellungen zu speichern.

8 Erweitert

Sicherung und Wiederherstellung

Das PRG AV4202N ermöglicht die Sicherung von Nutzer- und Systemdaten auf externen USB-Festplatten, die mit dem Router verbunden sind. Sie können automatische Sicherungen zu voreingestellten Zeiten festlegen.

Um den Sicherungsmechanismus zu aktivieren, muss der File Server aktiviert und konfiguriert sein sowie aus mindestens zwei Festplatten bestehen.

→ Der File Server muss aktiviert und konfiguriert sein.
→ Der File Server muss aus mindestens zwei Festplatten bestehen.

Bitte beachten Sie, dass die Sicherung auf Verzeichnisebene durchgeführt wird. Das bedeutet, dass es nicht möglich ist, eine einzelne, unabhängige Datei zu sichern.

1. Zu den Sicherungseinstellungen gelangen Sie entweder mit dem Link „Erweitert" in der Kategorie „Dienste" oder indem Sie auf das Symbol „Sicherung und Wiederherstellen" auf der Seite „Erweitert" klicken. Die Seite „Sicherung und Wiederherstellen" öffnet sich.

2. Klicken Sie auf den Link „Neuer Eintrag" im Abschnitt „Sicherungsterminierung".

3. Auf der Seite „Sicherung bearbeiten", die daraufhin erscheint, konfigurieren Sie die folgenden Parameter:
   → Geben Sie die Quelle für die Sicherung an. Zum Beispiel: A/homes.
   → Geben Sie den Zielort für die Sicherungsdateien an. Zum Beispiel: B/backups. Es wird empfohlen, als Zielort ein externes Speichergerät einzusetzen.
   → Wählen Sie gesamte Sicherung, schrittweise Sicherung oder beides, indem Sie den Zeitpunkt für die Sicherung angeben. Sie können zwischen täglichen, wöchentlichen oder monatlichen Sicherungen in den Comboboxen „Terminierung" wählen.

4. Drücken Sie auf „OK", um die Terminierungseinstellungen zu speichern.

5. Drücken Sie auf „Jetzt sichern", um die Sicherung sofort zu starten. Während der Sicherung zeigt der Bildschirm Status und Fortschritt der Sicherung.

Um Ihre Daten wiederherzustellen:

1. Drücken Sie auf das Symbol „Sicherung und Wiederherstellen" auf der Seite „Erweitert" der Verwaltungskonsole. Die Seite „Sicherung und Wiederherstellen" öffnet sich.

2. Drücken Sie auf „Wiederherstellen".

3. Auf der Seite „Wiederherstellen", die daraufhin erscheint, konfigurieren Sie die folgenden Parameter:
   - Geben Sie die Quelle, die wiederhergestellt werden soll, im Feld „Quelle Archiv" an. Zum Beispiel: A/homes.
   - Wählen Sie in der Combobox „Wiederherstellen", ob das gesamte Archiv oder nur ein Unterverzeichnis wiederhergestellt werden soll. Wenn Sie ein Unterverzeichnis wählen, erscheint ein zweites Feld, in das Sie den Namen des Unterverzeichnisses eingeben müssen.
     Zum Beispiel: Um A/homes/john wiederherzustellen, geben Sie john als Unterverzeichnis ein.
   - Wählen Sie einen Zielort, in welchem Sie Sie das Archiv wiederherstellen wollen. Sie können zwischen dem ursprünglichen Ort oder jedem anderen Verzeichnis wählen. Wenn Sie ein anderes Verzeichnis wählen, erscheint ein zweites Feld, in das Sie den Namen des Verzeichnisses eintragen müssen. Beachten Sie, dass der Pfad des wiederhergestellten Verzeichnisses unter dem Pfad des Zielverzeichnisses erstellt wird. Wenn Sie also das Verzeichnis „A/restore dir" angeben, ist das Ergebnis „A/restore dir/A/homes/john."

8 Erweitert

Universal Plug and Play

Universal Plug and Play ist eine Netzwerkarchitektur, die Kompatibilität unter Netzwerkgeräten, Software und Peripheriegeräten ermöglicht. Universal Plug-and-Play-fähige Produkte können nahtlos mit anderen UPnP-fähigen Geräten ohne Nutzerkonfiguration, zentralisierten Servern oder produktspezifischen Gerätetreibern verbunden werden und kommunizieren.

Wenn auf Ihrem Computer ein Betriebssystem läuft, das UPnP unterstützt, wie zum Beispiel Windows XP, können Sie den Computer Ihrem Heimnetzwerk hinzufügen und auf die webbasierte Verwaltung direkt von Windows aus zugreifen.

Wake up on LAN

Das PRG AV4202N ermöglicht Ihnen, Ihren PC aus einem abgeschalteten Softwarestatus über Fernzugriff „aufzuwecken", damit er sich mit der Homepage des Routers verbindet und auf die Funktion „Wake Up On LAN" zugreift. Sie sollten die Wake-up-on-LAN-Option im Konfigurationsfenster der Netzwerkoberfläche konfigurieren, um diese Funktion zu aktivieren. Im Abschnitt Wake Up on LAN Ihres PRG AV4202N müssen Sie die Schnittstelle wählen, die Sie verwenden möchten und die MAC-Adresse des PCs, der „aufgeweckt" werden soll.

8 Erweitert

Webserver

Das PRG AV4202N kann als Webserver agieren und eine oder mehrere Webseiten hosten, die vom LAN oder WAN aus erreichbar sind.

- Die Webseite wird auf dem PRG AV4202N gehostet, so dass keine Station im LAN als Webserver fungieren muss oder teure Hostdienste ausgelagert werden müssen.
- LAN-Sicherheit: Nutzer aus dem Internet können auf Ihre Webseite zugriffen, ohne Ihr LAN betreten zu müssen.
- Einfache und schnelle Konfiguration wird ermöglicht.

Um den Webserver zu konfigurieren, füllen Sie die folgenden Felder aus:

- **Enabled** (Aktiviert). Wählen Sie diese Funktion an oder ab, um sie zu aktivieren oder deaktivieren.
- **WAN Access** (Zugriff). Wählen Sie diese Checkbox, um Zugriff auf Ihren Webserver über das Internet zu erlauben.
- **Log Requests** (Log-Anfragen). Wählen Sie diese Checkbox, um Verbindungsanfragen, die Ihrem Webserver gesendet zu werden, zu loggen.
- **HTTP Port.** Der Port, den Ihr Webserver für HTTP-Datenverkehr verwendet.
- **HTTPS Port.** Der Port, den Ihr Webserver für HTTPS-Datenverkehr verwendet.
- **Data Allocation** (Datenzuordnung). Geben Sie den Pfad des Dateisystems des PRG-AV4202N-Ordners an, der den Inhalt Ihrer Webseite enthält.

Jeder Nutzer im LAN kann eine private Webseite konfigurieren, die man über http://openrg.home/~<username> erreichen kann. Dieser Pfad wird auf ein Unterverzeichnis des Homeverzeichnisses des Nutzers auf dem PRG AV4202N abgebildet. Um eine private Webseite einzurichten:

1. Überprüfen Sie, dass die Option „Nutzer Homeverzeichnis“ auf der Seite Nutzerkonteneinstellungen aktiviert ist (weitere Informationen erhalten Sie in Abschnitt 6.3.1).

2. Im Abschnitt „Nutzer Private Webseite“ der Seite „Webserver“ wählen Sie die Option „Aktiviert“.

3. Im Feld „Datenort“ geben Sie das Unterverzeichnis des Nutzers ein, das den Inhalt der Webseite enthält.

4. Klicken Sie auf „OK“, um die Einstellungen zu speichern.

Sie können eine beliebige Anzahl zusätzlicher Webseiten auf dem PRG-AV4202N-Webserver konfigurieren. Jede dieser Seiten wirkt, als wäre sie auf einem eigenen Host lokalisiert. Diese Methode wird als virtuelle Hosts bezeichnet. Zusätzlich können Sie eine beliebige Anzahl an Aliasen jedem virtuellen Host hinzufügen. Browser innerhalb des LANs erreichen Ihre Webseiten direkt. Sie können aber auch externen Zugang auf Ihre Seiten gewähren. Dazu müssen Sie Domainnamen registrieren. Achtung: Da die WAN-IP-Adresse dynamisch ist und sich bei jeder neuen Verbindung ändert, kann diese Funktion nur über DDNS gelöst werden. Nähere Informationen dazu finden Sie auf Seite 51.

8 Erweitert

Um zusätzliche Webseiten zu konfigurieren:

1. Klicken Sie unter „Virtuelle Hosts“ auf der Seite „Webserver“ auf „Neuer Eintrag“.

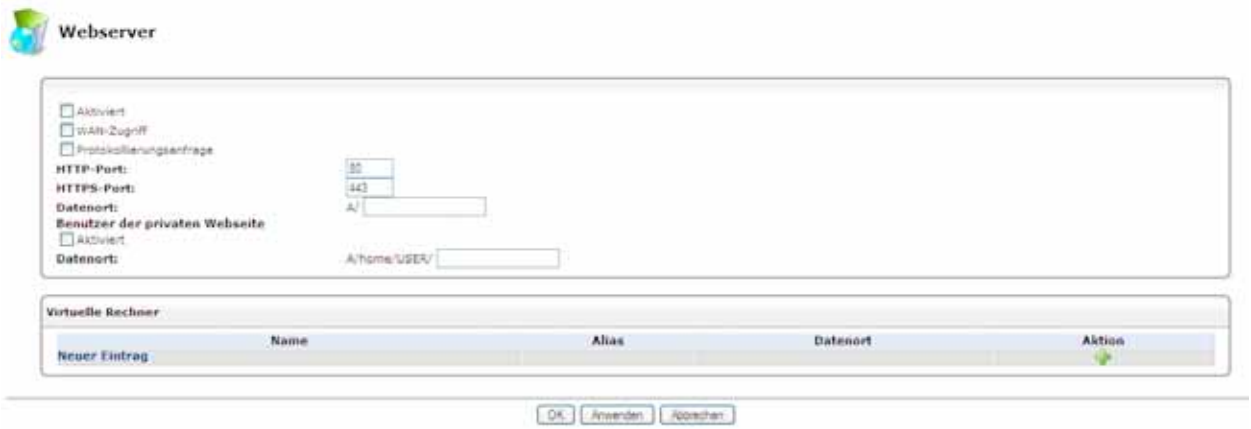
2. Geben Sie im Feld „Servername“ den Domainnamen der Webseite ein.

3. Geben Sie im Feld „Datenort“ den Pfad das Dateisystems zum PRG AV4202N-Ordner ein, der den Inhalt der Webseite enthält.

4. Um einem virtuellen Host einen Alias hinzuzufügen, klicken Sie auf „Neuer Eintrag“ im Bereich „Aliases.“

5. Geben Sie eine Alias-URL im Feld „Alias“ ein und klicken Sie auf „OK“. Der neue Alias erscheint im Abschnitt „Aliases“.

6. Klicken Sie auf „OK‘, um die Einstellungen zu speichern. Die URL und Aliase Ihrer Seite werden zum Abschnitt des Webservers „Virtuelle Hosts“ hinzugefügt.



Werkseinstellungen wiederherstellen

Wenn Sie die werksseitig vorgegebene Standardkonfiguration wiederherstellen wollen, weil Sie ein neues Netzwerk aufbauen möchten oder aus sonstigen Gründen:

1. Klicken Sie auf das Symbol „Standards wiederherstellen“ auf der Seite „Erweitert“ der webbasierten Verwaltung. Die Seite „Standards wiederherstellen“ erscheint.

2. Drücken Sie auf „OK“, um die Werkseinstellungen des Routers wiederherzustellen.

9 Systemüberwachung

Die Systemüberwachung ist über die Homepage des PRG AV4202N nach einer Nutzerauthentifizierung am Router verfügbar.

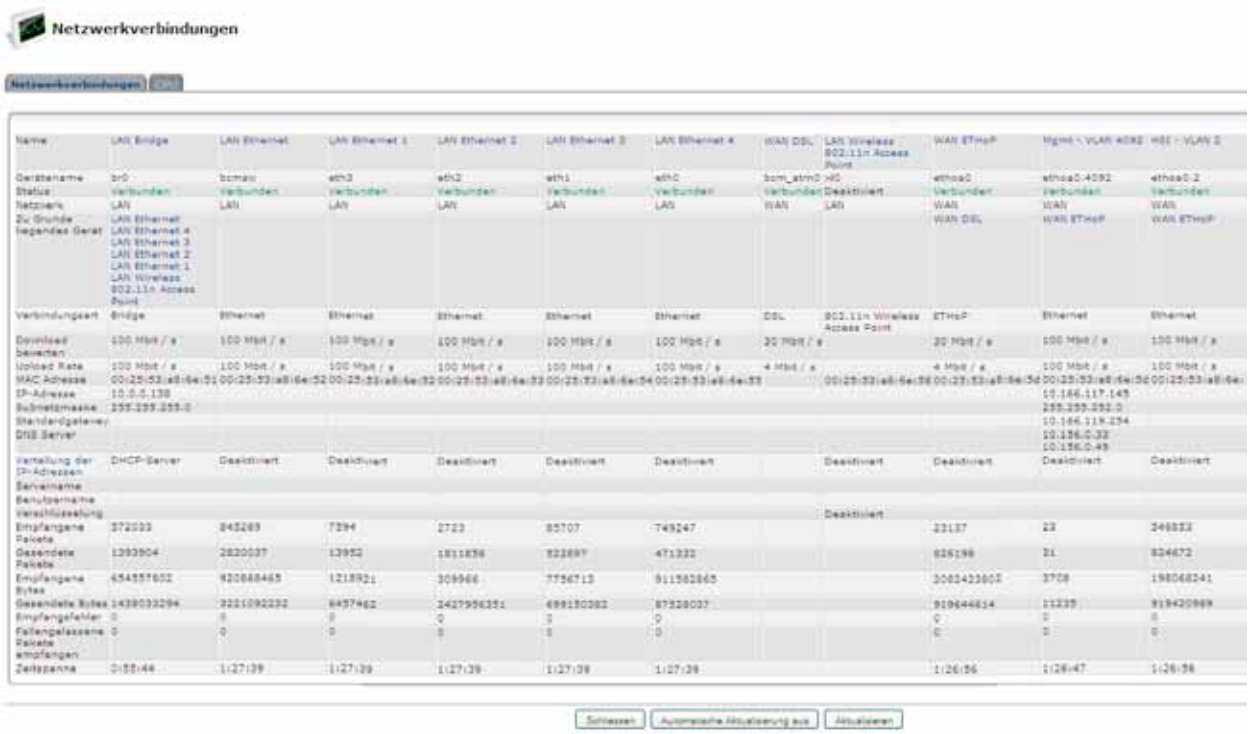
Beachten Sie bitte, dass jede Änderung der Konfiguration Ihre Konnektivität beeinträchtigen kann!

Network Connections (Netzwerkverbindungen)

Der Überwachungsbildschirm zeigt eine Tabelle, die einen Überblick über die überwachten Verbindungsdaten gibt. Der Pirelli PRG AV4202N überwacht kontinuierlich den Datenverkehr innerhalb des lokalen Netzwerks sowie zwischen dem lokalen Netzwerk und dem Internet.
Sie können statistische Angaben zu den Daten, die vom und zum Internet (WAN) sowie von und zu den Computern im lokalen Netzwerk (LAN) empfangen und gesendet wurden, abrufen.
Klicken Sie auf „Erneuern", um die Anzeige zu aktualisieren oder drücken Sie auf „Automatische Erneuerung An", um die angezeigten Parameter kontinuierlich zu aktualisieren.

Systemlog

Die Bildschirmseite „Log" zeigt eine Liste der aktuellen Aktivitäten, die auf dem Router stattgefunden haben.



9 Systemüberwachung

CPU

Die „CPU"-Bildschirmseite zeigt die Zeit an, die verstrichen ist, seit das System zuletzt gestartet wurde, sowie die Durchschnittsauslastung. Zusätzlich zeigt die Seite eine Liste aller Prozesse, die aktuell auf dem Router laufen, und ihren Verbrauch an virtuellem Speicher. Die Seite wird standardmäßig automatisch aktualisiert. Sie können dies jedoch ändern, indem Sie auf „Automatische Erneuerung Aus" klicken.

10 Problembehebung

Grundlegende Verbindungstests

- Überprüfen Sie, ob der Router mit Ihren Computern und der Telefonleitung verbunden ist und alle Geräte eingeschaltet sind. Prüfen Sie, ob die Kontrolllampen für den LAN- oder USB-Status (entsprechend Ihrer Verbindungsart) und für DSL auf dem Router leuchten und alle entsprechenden LEDs auf der NIC ebenfalls leuchten.
- Stellen Sie sicher, dass die Computer komplett hochgefahren und betriebsbereit sind. Einige Netzwerkschnittstellen sind möglicherweise nicht richtig initialisiert, bis die Computer komplett hochgefahren sind.
- Wenn die LED für den Linkstatus eines verbundenen Ports nicht leuchtet, kontrollieren Sie, ob ein Kabel defekt ist. Verwenden Sie ggf. ein anderes Kabel.

Browsen zu den Konfigurationsbildschirmseiten des Routers

Wenn Sie Ihren Router und Ihre Computer miteinander verbunden haben, aber nicht zu den Konfigurationsbildschirmseiten des Routers browsen können, überprüfen Sie Folgendes:

- Prüfen Sie, ob die physische Verbindung zwischen Ihrem Computer und dem Router in Ordnung ist und dass die LEDs für den LAN-Status auf dem Router und der NIC leuchten. Einige NICs haben keine Statuskontrolllampen. In diesem Fall könnte ein Diagnoseprogramm diese Informationen liefern.
- Kontrollieren Sie, ob Sie Ihren Computer, wie im Abschnitt „Installation Ihres Computers" ab Seite 12 beschrieben, konfiguriert haben. Starten Sie Ihren Computer neu, während er am Router angeschlossen ist, um sicherzustellen, dass er eine IP-Adresse erhält.
- Wenn Sie die Adresse Ihres Routers in Ihren Webbrowser eingeben, achten Sie darauf, dass Sie die komplette URL eingeben, einschließlich "http://" (z.B. http://10.0.0.138).
- Überprüfen Sie, dass Sie z. B. keinen Web-Proxy auf Ihrem Computer aktiviert haben. Gehen Sie zur Steuerungsseite und klicken Sie auf Internetoptionen. Wählen Sie „Verbindungen" und klicken Sie auf LAN-Einstellungen unten auf der Seite. Vergewissern Sie sich, dass die Option Proxy Server nicht gewählt ist. Wenn Sie nicht bis zum Router browsen können, verwenden Sie das Programm „winipcfg" in Windows 98/ME, um zu überprüfen, ob Ihr Computer die richtigen Adressdaten vom Router bekommt. Wählen Sie im Startmenü „Start" und geben Sie dann „winipcfg" ein. Kontrollieren Sie, ob der Computer eine IP-Adresse in der Form 10.0.0.xxx hat (wobei xxx zwischen 1-137 oder 139-254 liegt), die Subnetzmaske 255.255.255.0 und der Standard-Router 10.0.0.138 ist (die Adresse des Routers). Wenn diese Daten nicht stimmen, benutzen Sie die Funktionen „Freigabe" und „Erneuern", um eine neue IP-Adresse vom Router zu bekommen. Unter Windows 2000, Windows XP, Vista und Windows 7 verwenden Sie die Befehlszeilenfunktion „ipconfig", um die gleichen Funktionen auszuführen.

Mit dem Internet verbinden

Wenn Sie bis zu den Konfigurationsseiten des Routers browsen können, aber nicht auf die Internetseiten gelangen, überprüfen Sie Folgendes:

- Kontrollieren Sie, ob die physische Verbindung zwischen Router und Telefonleitung in Ordnung ist und dass die DSL-LED auf dem Router weiß leuchtet.
- Stellen Sie sicher, dass Sie die richtigen Angaben auf den Konfigurationsseiten des Routers wie benötigt eingegeben haben. Kontrollieren Sie dies in den „Interneteinstellungen".
- Prüfen Sie, ob der Benutzername und das Passwort richtig sind.
- Stellen Sie sicher, dass Ihr Computer keinen Web-Proxy verwendet. Auf Windows-Computern kann dies unter Steuerung → Internetoptionen → Verbindungen überprüft werden.

10 Problembehebung

Vergessenes Passwort und Zurücksetzen auf Werkseinstellungen

Wenn Sie zu den Konfigurationsseiten des Routers browsen, sich aber nicht anmelden können, weil Sie das Passwort nicht kennen oder vergessen haben, gehen Sie wie folgt vor, um den Router auf seine Werkeinstellungen zurückzusetzen:

Alle Änderungen Ihrer Konfigurationen gehen verloren und Sie müssen Ihr Netzwerk neu konfigurieren, bevor Sie Ihren Router wieder mit dem Internet verbinden können. Außerdem werden auch die anderen Computernutzer vom Netzwerk getrennt, während dieser Vorgang stattfindet. Sie sollten daher einen entsprechend geeigneten Zeitpunkt für die Konfiguration wählen.

1. Schalten Sie den Router aus.
2. Trennen Sie alle Computer und die Telefonleitung vom Router.
3. Schalten Sie den Router wieder ein und warten Sie, bis er vollständig hochgefahren ist.
4. Drücken Sie ein paar Sekunden lang die Reset-Taste auf der Rückseite.
5. Der Router startet neu. Wenn der Startvorgang abgeschlossen ist, browsen Sie zu: „http://10.0.0.138“ und konfigurieren Ihr Netzwerk.
6. Schließen Sie Ihr Netzwerk wieder wie zuvor an.

Drahtlose Vernetzung

- Stellen Sie sicher, dass Sie einen Drahtlosadapter 802.11b/g oder 802.11n für jeden drahtlosen Computer haben und dass er korrekt installiert und konfiguriert ist. Überprüfen Sie, ob auf jedem drahtlosen Computer entweder Windows 98SE oder höher oder MAC OS 10.x oder höher installiert ist.
- Wenn Sie eine verkabelte und eine drahtlose NIC im gleichen Computer haben, stellen Sie sicher, dass die verkabelte NIC deaktiviert ist.
- Kontrollieren Sie die LED für den Drahtlosstatus des Routers.
- Stellen Sie sicher, dass die TCP/IP-Einstellungen für alle Geräte korrekt sind.
- Stellen Sie sicher, dass die drahtlosen Clients die gleiche SSID oder die gleichen Dienstbereichsnamen wie der Router benutzen. Bei der SSID müssen Sie die Groß- und Kleinschreibung beachten.
- Stellen Sie sicher, dass die Verschlüsselungsmethode und die Ebene, die Sie auf Ihren Clients verwenden, die gleichen sind wie auf dem Router. Der Router kann nicht gleichzeitig WPA- und WEP-Verschlüsselungen unterstützen.
- Stellen Sie sicher, dass Sie den drahtlosen Computer in der Liste der zugelassenen MAC-Adressen aktiviert haben, wenn Sie die MAC-Adressfilterung auf dem Router verwenden.
- Wenn Sie Schwierigkeiten haben, bei niedriger Geschwindigkeit eine Verbindung herzustellen oder zu arbeiten, können Sie den drahtlosen Computer näher an den Router stellen, um sicherzustellen, dass die Gebäudestruktur oder Einrichtungen die Konnektivität nicht beeinträchtigt. Wenn damit das Problem behoben ist, sollten Sie den Aufstellungsort des drahtlosen Computers oder des Routers entsprechend ändern oder einen anderen Kanal für den Router verwenden.

- Störquellen: Das 2.4-GHz-ISM-Band wird verwendet für 802.11b/g und 802.11n. Dies ist im Allgemeinen ein lizenzfreies Band für Niedrigstromanwendungen. Ggf. haben Sie weitere Geräte, die in diesem Frequenzband betrieben werden. Sie sollten sicherstellen, dass keine Geräte wie zum Beispiel Mikrowellenöfen in der Nähe des Routers oder der drahtlosen Computer stehen, da dies den Betrieb des Empfängers beeinträchtigen und die Leistung Ihres Netzwerks reduzieren könnte. Versuchen Sie, wenn Probleme auftreten, sowohl die drahtlosen Computer als auch den Router umzustellen.
- Die meisten Drahtlosadapter für Computer suchen die Kanäle nach dem drahtlosen Router ab. Wenn ein drahtloser Computer den Router nicht finden kann, versuchen Sie, die Suche manuell zu starten, wenn die Client-Software diese Funktion unterstützt, oder stellen Sie den Kanal manuell auf Ihrem drahtlosen Computer entsprechend dem Kanal des Routers ein. Nähere Informationen finden Sie in der Gebrauchsanweisung des Drahtlosadapters und in den Hinweisen Ihres Anbieters.
- Verbindungsgeschwindigkeit: Die Standards 802.11b/g und 802.11n wählen automatisch die optimale Geschwindigkeit, abhängig von der Qualität Ihrer Verbindung. Wenn die Signalqualität schwächer wird, geht die Geschwindigkeit zurück. Die von 802.11g unterstützten Geschwindigkeiten sind 54 Mbits, 48 Mbits, 36 Mbits, 24 Mbits, 18 Mbits, 12 Mbits, und 6 Mbits. Die von 802.11b unterstützten Geschwindigkeiten sind 11 Mbits, 5.5 Mbits, 2 Mbits und 1 Mbits. Der 802.11n unterstützt bis zu 100 Mbits. Im Allgemeinen ist die Geschwindigkeit besser, je näher Sie am Router sind. Wenn Sie die erwartete Geschwindigkeit nicht erreichen, versuchen Sie, den drahtlosen Computer näher an den Router zu stellen. In einem idealen Netzwerk befindet sich der Router in der Mitte und die drahtlosen Computer sind um ihn herum platziert. Anwendungen, die eine Lagebewertung vornehmen, sind im Allgemeinen mit der drahtlosen Computerkarte erhältlich. Verwenden Sie diese Funktion, um den optimalen Platz für Ihren drahtlosen Computer zu finden. Weitere Informationen finden Sie in der Gebrauchsanweisung zu Ihrer Computerkarte und den Hinweisen Ihres Anbieters.

Häufig gestellte Fragen

Wie stelle ich den Router auf die Werkseinstellungen zurück?
Siehe Abschnitt „Vergessenes Passwort und Zurücksetzen auf Werkseinstellungen".

Wie viele Computer werden vom Router im LAN unterstützt?
Bis zu 256 Computer.

Die Dienstqualität (QoS) ist verbunden mit dem garantierten Niveau des Durchsatzes (die Datenmenge, die vom Router an die Clients übertragen wird). Je mehr Clients verbunden sind, desto niedriger ist die Dienstqualität.

Wie viele drahtlose Clients werden vom Router unterstützt?
Es werden 15 drahtlose Clients unterstützt.

Wie werden zusätzliche Computer angeschlossen?
Sie können die Anzahl der in Ihrem LAN verfügbaren Verbindungen erweitern, indem Sie Hubs, Switches und drahtlose Access Points benutzen, um sie mit dem Router zu verbinden. Drahtlose Access Points, Hubs und Switches sind eine einfache und zuverlässige Methode, um Ihr Netzwerk zu erweitern. Ihr Anbieter informiert Sie gerne im Detail.

11 Sicherheitshinweise

Wichtige Sicherheitshinweise
Dieser Anhang enthält Anweisungen, die Sie zum Schutz Ihrer persönlichen Sicherheit befolgen müssen. Befolgen Sie alle Anweisungen genau. Sie sollten die folgenden Sicherheitshinweise sorgfältig lesen, bevor Sie die Anlage installieren oder entfernen.

Verwenden Sie nur das Netzteil, das mit dem Gerät geliefert wird. Die Verwendung von anderen Netzteilen kann den Router beschädigen und zu einem Verfall der Garantie führen.

- Verwenden Sie eine Steckdose in Reichweite und achten Sie darauf, dass das Stromkabel nicht beschädigt wird.
- Um einen Stromschlag zu vermeiden, sollten Sie den Router nicht öffnen.
- Um Brand- oder Stromschlaggefahren zu vermeiden, sollte Ihr Router weder mit Regen, Feuchtigkeit, Flüssigkeiten noch toxischen Substanzen in Kontakt kommen.
- Berühren Sie niemals unisolierte Telefonkabel oder Anschlüsse, wenn die Telefonleitung nicht zuvor von der Netzwerkschnittstelle getrennt wurde.
- Stellen Sie eine korrekte Belüftung des Routers sicher. Blockieren Sie nicht die Lüftungsöffnungen des Geräts und stellen Sie keine Gegenstände darauf.
- Stellen Sie Ihren Router nicht ins direkte Sonnenlicht und nicht in die Nähe von Wärmequellen.
- Verwenden Sie Ihren Router nicht während eines Gewitters.
- Der Router erzeugt und verwendet Funkfrequenz(RF)-Energie. In Österreich ist dieser Router ohne Einschränkung zugelassen.

Das durchgekreuzte Mülltonnensymbol auf einem elektrischen oder elektronischen Gerät oder seiner Verpackung weist darauf hin, dass es am Ende
seiner Betriebsdauer nicht als unsortierter Hausmüll entsorgt werden darf.

Als Verbraucher müssen Sie deshalb die spezielle Wertstoffentsorgung und insbesondere die städtische Abfallentsorgung für die Entsorgung elektrischer und elektronischer Geräte beachten.

Eine getrennte und umweltbewusste Entsorgung des Geräts hilft, natürliche Ressourcen zu erhalten und schützt Mensch und Umwelt vor etwaigen gesundheitsschädlichen Bestandteilen, Materialen und Substanzen.

Eine professionelle, umweltbewusste Entsorgung des Geräts ermöglicht ggf. außerdem eine Wiederverwertung.

12 IP-Adressierung

Die Internetprotokollfamilie

Die Internetprotokollfamilie besteht aus einem klar definierten Satz an Netzwerkprotokollen und verschiedenen herkömmlichen Anwendungsprotokollen. Das Transmission Control Protocol/Internetprotokoll (TCP/IP) ist wahrscheinlich das bekannteste Protokoll und eine Kombination der beiden Protokolle (IP und TCP), die zusammenarbeiten. TCP/IP ist ein international anerkannter und unterstützter Netzwerkstandard, der eine Konnektivität zwischen Geräten von verschiedenen Anbietern über eine große Anzahl an Vernetzungstechnologien bietet.

Verwaltung des Routers über das Netzwerk

Um ein Gerät über das Netzwerk zu verwalten, muss der Router korrekt mit den folgenden IP-Angaben konfiguriert sein:

- IP-Adresse
- Subnetzmaske

IP-Adressen und Subnetzmasken

Jedes Gerät in Ihrem Netzwerk muss eine eigene IP-Adresse haben, um richtig funktionieren zu können. Eine IP-Adresse ermittelt die Adresse des Geräts, zu dem Daten gesendet werden, und die Adresse des Zielnetzwerks. IP-Adressen haben das Format n.n.n.x, wobei n für eine Dezimalzahl zwischen 0 und 255 und x für eine Zahl zwischen 1 und 254 (einschließlich) steht. Jedoch reicht eine IP-Adresse allein nicht aus, damit Ihr Gerät funktioniert. Zusätzlich zur IP-Adresse ist eine Subnetzmaske erforderlich. Alle Netzwerke sind in kleinere Subnetzwerke unterteilt. Eine Subnetzmaske ist eine Zahl, die einem Gerät ermöglicht, das Subnetzwerk zu erkennen, mit dem es verbunden ist.

Damit Ihr Netzwerk korrekt funktioniert, müssen alle Geräte Ihres Netzwerks Folgendes besitzen:

- die gleiche Subnetzwerkadresse
- die gleiche Subnetzmaske

Der einzige Wert, der sich unterscheidet, ist die spezielle Host-Gerätenummer. Dieser Wert darf stets nur einmal vergeben werden.

Ein Beispiel für eine IP-Adresse ist „192.168.10.8." Die Größe des Netzwerks bestimmt den Aufbau dieser IP-Adresse. Bei der Verwendung Ihres Routers werden Sie möglicherweise auf zwei Arten von IP-Adressen und Subnetzmaskenstrukturen stoßen.

Typ eins
In einem kleinen Netzwerk wird die IP-Adresse „192.168.10.8" in zwei Teile unterteilt:

- Teil eins („192.168.10") erkennt das Netzwerk, zu dem das Gerät gehört.
- Teil zwei („.8") ermittelt das Gerät innerhalb des Netzwerks.

Dieser Typ einer IP-Adresse funktioniert auf einer Subnetzmaske von „255.255.255.0."

Typ zwei
In größeren Netzwerken, in denen es mehrere Geräte gibt, wird die IP-Adresse „192.168.10.8" ebenso in zwei Teile aufgeteilt, ist aber unterschiedlich aufgebaut:

- Teil eins („192.168") ermittelt das Netzwerk, zu dem das Gerät gehört.
- Teil zwei („.10.8") erkennt das Gerät innerhalb des Netzwerks.

Dieser Typ einer IP-Adresse funktioniert auf einer Subnetzmaske von „255.255.0.0."

12 IP-Adressierung

Wie erhält ein Gerät eine IP-Adresse und eine Subnetzmaske?

Es gibt drei verschiedene Wege, um eine IP-Adresse und die Subnetzmaske zu erhalten:

- Dynamic-Host-Configuration-Protocol(DHCP)-Adressierung
- statische Adressierung
- automatische Adressierung (Auto-IP-Adressierung)

DHCP-Adressierung

Der Router enthält einen DHCP-Server, der es den Computern in Ihrem Netzwerk ermöglicht, eine IP-Adresse und Subnetzmaske automatisch zu beziehen. DHCP weist eine temporäre IP-Adresse und Subnetzmaske zu, die neu zugeteilt werden, wenn Sie sich vom Netzwerk trennen.

DHCP läuft auf jedem Client-Betriebssystem. Durch die Verwendung von DHCP werden niemals die gleiche IP-Adresse und Subnetzmaske zweimal für Geräte im Netzwerk vergeben. DHCP ist besonders geeignet für Netzwerke mit einer großen Anzahl an Nutzern.

Statische Adressierung

Sie müssen eine IP-Adresse und Subnetzmaske manuell für jedes Gerät eingeben. Die Verwendung einer statischen IP-Adresse und Subnetzmaske bedeutet, dass diese Adresse permanent festgelegt ist.

Auto-IP-Addressierung

Netzwerkgeräte verwenden die automatische IP-Adressierung, wenn sie so konfiguriert sind, dass sie eine Adresse über DHCP beziehen, aber keinen Kontakt zu einem DHCP-Server aufbauen können. Die automatische IP-Adressierung ist ein Modell, bei dem Geräte sich selbst eine IP-Adresse zufällig vom Subnetz des Industriestandards 169.254.x.x zuteilen (mit der Subnetzmaske 255.255.0.0). Wenn zwei Geräte sich die gleiche Adresse zuweisen, wird dies ermittelt und eines der Geräte weist sich eine neue Adresse zu. Die automatische IP-Adressierungshilfe wurde von Microsoft im Betriebssystem Windows 98 eingeführt und wird auch in Windows 2000 und Windows XP unterstützt.

Technische Daten des PRG AV4202N:

Schnittstellen/Standard

WAN-Schnittstelle

1 Leitungsport (RJ-11-Stecker, inneres Paar), der die folgenden Standards unterstützt:

- VDSL (G.993.2, G.993.2 Ergänzung 1, 2 und 3)
- ADSL (G.992.1, G992.2, T1.413, G994.1, G.997.1)
- ADSL2 (G.992.3)
- ADSL2+ (G992.5)

Anhang A/Anhang B sind in verschiedenen Produktversionen verfügbar.

LAN-Schnittstelle

- 4 10/100BASE-T Ethernet Ports (RJ-45 Stecker), IEEE 802.3, kompatibel mit Auto MDIX und Autonegotiation
- Ports können konfiguriert werden, um für Videodatenverkehr zu/von einem STB dediziert zu werden
- 2 USB Host v.2.0

Wireless-LAN-Schnittstelle

Wi-Fi Access Point ist kompatibel mit folgenden Standards:

- IEEE 802.11b/g/n
- WPA/WPA2 (IEEE 802.11i)
- WMM (IEEE 802.11e)

Sprachschnittstelle

- 2 FXS-Telefonanschlüsse (RJ-11-Stecker)

DSL(ATM)-Eigenschaften

- AAL5 (ITU-T I.363.5)
- UBR, VBR-nrt, VBR-rt, CBR-Datenverkehrsklassen
- mehrere VC/PPP-Anschlüsse
- klassische IP (CLIP) und ARP über ATM, RFCs 1577, 2225
- mehrere PPPoE-Anschlüsse auf einem einfachen VC
- Multi-Protocol Encapsulation über AAL5 Bridging und Routing, RFCs 1483, 268
- PPP über AAL5 (PPPoATM), RFC 2364
- OAM (ITU-T I.610)
- F4, F5
- Prüfschleife
- Encapsulation Modi in ATM Stapel: LLC und VC-Mux

13 Technische Daten

Routing/Bridging

Routing:
- statisches Routing
- RIPv1, RIPv2
- IP Multicasting – IGMP v2, v3

Bridge:
- WAN-LAN transparentes Bridging
- transparentes Bridging zwischen LAN-Geräten
- automatische Ermittlung von MAC-Adressen
- Spanning Tree Protocol

NAT

- NAT-NAPT, RFCs 3022
- statisches NAT
- statisches NAPT
- Application Level Gateway (ALGs) Modul

QoS

- ATM QoS: UBR, VBR-nrt, VBR-rt, CBR
- 802.1P/Q Priorisierung
- Diffserv(RFC2474, RFC2475)-Kennzeichnung und Warteschlangenbildung je nach Verbindungsart, Netzwerkschnittstelle, MAC, IP, Hostname, DSCP/ToS-Wert, Portanzahl und Anwendung
- Port basiertes QoS

Fernwartung

DSL-Forum-TR-069-CPE-Management-Protokoll:
- Autokonfiguration und Dynamic Service
- Software/Firmware Image Management
- Status- und Performance-Überwachung
- WEB GUI (HTTP-S Webserver)
- TFTP, RFC 1350
- Telnetserver

13 Technische Daten

Sicherheit

- Stateful Packet Inspection (SPI) Firewall
- IP-Protokollfilterung
- Zugangskontrolle
- Kindersicherung

Umgebungsspezifikationen

Temperatur:
- im Betrieb: +0° bis 40° C
- ohne Betrieb: unter 0°C und über 40°C

Relative Luftfeuchtigkeit:
- im Betrieb: 10 % bis 85 % nicht kondensierend
- ohne Betrieb: unter 10 % und über 85 % nicht kondensierend

Stromadapter

- europäischer Stecker
- Primär: Nennspannung 220V-230V, 50 Hz;
- Sekundär: 12V 2A

13 Technische Daten

Konformitätserklärung

Wir, Pirelli BroadBand Solutions SpA, Viale Sarca, 222, 20126 Mailand, www.Pirelli.com, Iltalien, erklären uns zuständig und verantwortlich dafür, dass das Produkt PRG AV4202N (P/N 151046301), auf das sich diese Erklärung bezieht, mit den zutreffenden Standards gemäß der Regelung in Artikel 3.1.a, 3.1.b und 3.2 der R&TTE Richtlinie 1999/5/EEC der Europäischen Gemeinschaft übereinstimmt.

Angewandte Standards:
- EN 55022
- EN 61000-3-2
- EN 61000-3-3
- EN 301 489-1
- EN 301 489-17
- EN 300 328
- EN 60950-1

Öffentliche Behörden wurden gemäß Artikel 6.4 der Frequenzbenachrichtigung informiert. Besondere Anforderungen wurden berücksichtigt. Das Produkt besitzt die CE-Kennzeichnung.

Jede ungenehmigte Veränderung des Produkts macht diese Erklärung ungültig. Dieses Produkt kann in folgenden Ländern verwendet werden:

AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU,
MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

13 Technische Daten

Entsorgung von elektrischen und elektronischen Geräten (WEE)

Dieses Produkt erfüllt die Kennzeichnungsanforderung der Richtlinie WEEE (2002/96/EC). Die aufgeklebte Produktkennzeichnung (siehe oben) weist darauf hin, dass Sie dieses elektrische / elektronische Produkt nicht im Hausmüll entsorgen dürfen.

Produktkategorie: Mit Bezug auf die Gerätetypen in der Richtlinie WEEE Anhang 1 ist dieses Produkt als „IT- und Telekommunikationsgerät" eingestuft.

Nicht im Hausmüll entsorgen.

14 Glossar

802.11b

Die IEEE-Spezifikation für drahtloses Ethernet ermöglicht Übertragungsraten von bis zu 11 Mbits. Der Standard definiert Übertragungsraten von 1, 2, 5.5 und 11 Mbits. Die Raten wechseln automatisch je nach Reichweite und Umgebung.

802.11g

Die IEEE-Spezifikation für drahtloses Ethernet ermöglicht Übertragungsraten von bis zu 54 Mbits. Der Standard definiert Übertragungsraten von 6, 12, 24, 36, 48 und 54 Mbits. Die Raten wechseln automatisch je nach Reichweite und Umgebung.

802.11n

Die IEEE-Spezifikation für drahtloses Ethernet ermöglicht Übertragungsraten von bis zu 100 Mbits.

10BASE-T

Die IEEE-Spezifikation für 10 Mbits Ethernet über Twisted-Pair-Kabel der Kategorie 3, 4 oder 5.

100BASE-TX

Die IEEE-Spezifikation für 100 Mbits Fast Ethernet über Twisted-Pair-Kabel der Kategorie 5.

Access Point

Ein Access Point ist ein Gerät, über das sich drahtlose Clients mit anderen drahtlosen Clients verbinden und das als Brücke zwischen drahtlosen Clients und einem drahtlosen Netzwerk, wie zum Beispiel Ethernet, dient. Drahtlose Clients können überall innerhalb des Empfangsgebiets des Access Points bewegt werden und sind immer noch miteinander verbunden. Bei einer Verbindung mit einem Ethernet-Netzwerk überwacht der Access Point den Ethernet-Verkehr und leitet entsprechende Ethernet-Nachrichten an das Drahtlosnetzwerk weiter, während es ebenso den Funkdatenverkehr der drahtlosen Clients überwacht und Nachrichten der drahtlosen Clients an das Ethernet-LAN weiterleitet.

Ad-hoc-Modus

Der Ad-hoc-Modus ist eine Konfiguration, die von den meisten drahtlosen Clients unterstützt wird. Er wird verwendet, um ein Peer-to-Peer-Netzwerk zu verbinden, ohne einen Access Point verwenden zu müssen. Er bietet eine geringere Leistung als der Infrastrukturmodus. Dies ist der Modus, den der Router verwendet (siehe auch Infrastrukturmodus).

Autonegotiation

Einige Geräte in diesem Produktbereich unterstützen die Autonegotiation. Autonegotiation bedeutet, dass zwei Geräte bei optimaler Geschwindigkeit einen Link teilen, und ist automatisch konfiguriert, um die beste gemeinsame Geschwindigkeit zu verwenden. Die bevorzugte Reihenfolge (beste zuerst) ist: 100BASE-TX vollduplex, 100BASE-TX halbduplex, 10BASE-T vollduplex und 10BASE-T halbduplex. Autonegotiation ist im Standard IEEE 802.3 für Ethernet definiert und findet in wenigen Millisekunden statt.

Bandbreite

Bandbreite ist die Datenkapazität, gemessen in Bits pro Sekunde, die ein Kanal übertragen kann. Die Bandbreite des Ethernet beträgt 10 Mbits, die Bandbreite eines Fast Ethernet 100 Mbits. Die Bandbreite für 802.11b drahtlos ist 11 Mbits.

14 Glossar

Kabel der Kategorie 5

Eine von 5 Kategorien bei Twisted Pair (TP)-Kabeln, die durch den EIA/TIA-586 Standard definiert sind. Kategorie 5 kann in Ethernet (10BASE-T) und Fast-Ethernet-Netzwerken (100BASE-TX) verwendet werden und Daten mit Raten von 100 Mbits übertragen. Kabel der Kategorie 5 sind für Netzwerke besser geeignet als die Kategorie 3, weil sie sowohl Übertragungen durch Ethernet (10 Mbits) als auch Fast Ethernet (100 Mbits) unterstützen.

Kanal

Ähnlich wie bei jedem Funkgerät ermöglicht der drahtlose Kabel-/DSL-Router, verschiedene Funkkanäle im drahtlosen Spektrum zu wählen. Ein Kanal ist eine bestimmte Frequenz innerhalb des 2.4 GHz Spektrums, innerhalb dessen der Router arbeitet.

Client

Desktop-PC, der mit dem Netzwerk verbunden ist.

DHCP

Dynamic Host Configuration Protocol. Dieses Protokoll weist automatisch jedem Computer in Ihrem Netzwerk eine IP-Adresse zu. Windows 95, Windows 98 und Windows NT 4.0 enthalten Software, die Arbeitsplatzrechnern in einem Netzwerk IP-Adressen zuteilt. Diese Zuteilungen werden von der DHCP-Server-Software vorgenommen, die auf Windows-NT-Servern läuft. Windows 95 und Windows 98 beziehen die Adresse vom Server. Windows 98 weist sich selbst eine Adresse zu, falls kein DHCP-Server gefunden werden kann.

DMZ

DMZ (Demilitarized Zone) ist ein Bereich außerhalb der Firewall, die es Fernnutzern ermöglicht, auf Funktionen Ihres Netzwerks zuzugreifen (Webseite, FTP Download und Upload-Bereiche etc.).

DNS-Server-Adresse

DNS steht für Domain Name System, das es Internet-Host-Computern ermöglicht, einen Domainnamen zu besitzen (zum Beispiel pirelli.com) sowie eine oder mehrere IP-Adressen (zum Beispiel 192.168.10.8). Ein DNS-Server pflegt eine Datenbank von Host-Computern und ihre entsprechenden Domainnamen und IP-Adressen, sodass, wenn ein Domainname aufgerufen wird (wie bei der Eingabe von „pirelli.com" in Ihrem Internetbrowser), der Nutzer zur richtigen IP-Adresse geleitet wird. Die DNS-Server-Adresse, die von den Computern Ihres Heimnetzwerks verwendet wird, ist der Ort des DNS-Servers, den Ihr ISP zugeteilt hat.

DSL

Kurz für Digital Subscriber Line (digitale Anschlussleitung), wird üblicherweise verwendet mit Bezug auf die asymmetrische Version dieser Technologie (ADSL), mit der Daten über bestehende Kupfertelefonleitungen mit Übertragungsraten von 1.5 bis 9 Mbps geschickt werden können, wenn Daten empfangen werden (bekannt als die Downstream-Rate) und von 16 bis 640 Kbps, wenn Daten gesendet werden (bekannt als die Upstream-Rate). ADSL erfordert ein spezielles ADSL-Modem. ADSL erfreut sich zunehmender Beliebtheit, da immer mehr Bereiche der Welt Internetzugang erhalten.

DSL-Modem

DSL steht für Digital Subscriber Line (siehe oben). Ein DSL-Modem verwendet Ihre bestehenden Telefonleitungen, um Daten mit Hochgeschwindigkeitsraten zu senden und zu empfangen.

14 Glossar

Verschlüsselung

Eine Methode, um drahtlose Datenübertragungen mit Sicherungsebenen zu schützen. Der Router verwendet zwei Verschlüsselungsebenen; 40/64 bit und 128 bit. 128 bit sind leistungsfähigere Verschlüsselungsebenen als 40/64 bit.

Ethernet

Eine LAN-Spezifikation, die gemeinsam von Xerox, Intel und Digital Equipment Corporation entwickelt wurde. Ethernet-Netzwerke verwenden CSMA/CD, um Datenpakete bei einer Rate von 10 Mbps über eine Vielzahl an Kabeln zu übertragen.

Ethernet-Adresse

Siehe MAC-Adresse.

Fast Ethernet

Ein Ethernet-System mit einer Datenübertragungsrate von 100 Mbps.

Firewall

Elektronischer Schutz, der Fremde außerhalb Ihres Netzwerks daran hindert, auf Ihre Dateien zuzugreifen und Ihren Computer zu beschädigen.

Vollduplex

Ein System, das es ermöglicht, Datenpakete gleichzeitig zu übertragen und zu empfangen und das den möglichen Durchsatz eines Links verdoppelt.

EEE

Institute of Electrical and Electronics Engineers. Diese amerikanische Organisation wurde 1963 gegründet und setzt die Standards für Computer und Kommunikation.

IETF

Internet Engineering Task Force. Eine Organisation, die dafür verantwortlich ist, Entwicklungslösungen für TCP/IP-Netzwerke zu liefern. Im Bereich des Netzwerkmanagements ist diese Gruppe zuständig für die Entwicklung des SNMP-Protokolls.

IGMP

Das Internet Group Management Protocol (IGMP) ist ein Internetprotokoll, das einem Internetcomputer eine Möglichkeit bietet, seine Multicast-Gruppenmitgliedschaft an benachbarte Router weiterzugeben. Multicasting ermöglicht einem Computer im Internet, Inhalte an andere Computer zu senden. Multicasting kann für Anwendungen wie die Aktualisierung der Adressbücher von mobilen Computernutzern verwendet werden, für das Verschicken von Unternehmens-Newslettern über eine Verteilerliste und für das „Senden" von Programmen hoher Bandbreite, um sie einem „eingeschalteten" Publikum zu zeigen, indem eine Multicast-Gruppenmitgliedschaft eingerichtet wird.

14 Glossar

Infrastrukturmodus

Der Infrastrukturmodus ist die vom Router unterstützte drahtlose Konfiguration. Sie müssen sicherstellen, dass alle Clients den Infrastrukturmodus eingestellt haben, damit sie mit dem in Ihrem Router eingebauten Access Point kommunizieren können (siehe auch Ad-hoc-Modus).

IP

Internetprotokoll. IP ist ein Layer-3-Netzwerkprotokoll, das der Standard für das Senden von Daten in einem Netzwerk ist. IP ist Teil des TCP/IP-Protokollpakets, welches das Routing von Datenpaketen an angesprochene Geräte beschreibt. Eine IP-Adresse besteht aus 32 bits, die in zwei oder drei Felder unterteilt werden: eine Netzwerknummer und eine Hostnummer oder eine Netzwerknummer, eine Subnetznummer und eine Hostnummer.

IP-Adresse

Internetprotokolladresse. Eine spezielle Kennzeichnung für ein Gerät, das zu einem Netzwerk gehört, indem es TCP/IP verwendet. Die Adresse wird als vier Achtergruppen, getrennt durch Punkte (Satzzeichen), geschrieben und besteht aus einem Netzwerkabschnitt, einem optionalen Subnetzabschnitt und einem Host-Abschnitt.

ISP

Internet Service Provider. Ein ISP ist ein Unternehmen, das eine Verbindung zum Internet für Privatpersonen, Unternehmen und Organisationen anbietet.

LAN

Local Area Network (lokales Netzwerk). Ein Netzwerk mit Endgeräten (zum Beispiel PCs, Drucker, Server) und Netzwerkgeräten (Hubs und Switches), die einen relativ kleinen geografischen Bereich decken (normalerweise nicht größer als ein Stockwerk oder Gebäude). LANs zeichnen sich durch hohe Übertragungsraten über geringe Distanzen aus (bis zu 1000 Meter).

MAC

Media Access Control. Ein von der IEEE spezifiziertes Protokoll, um zu bestimmen, welche Geräte zu welcher Zeit Zugang zum Netzwerk haben.

MAC Adresse

Media Access Control Address. Auch Hardware- oder physikalische Adresse genannt. Eine Layer-2-Adresse in Verbindung mit einem bestimmten Netzwerkgerät. Die meisten Geräte, die an ein LAN gebunden sind, haben eine MAC-Adresse, die ihnen zugeteilt wurde, um andere Geräte im Netzwerk zu ermitteln. MAC-Adressen sind 6 Bytes lang.

Mbps

Megabits pro Sekunde.

MDI/MDIX

Bei der Verkabelung geht das Konzept des Sendens und Empfangens von der Perspektive des PCs aus, der als Media Dependant Interface (MDI) (medienabhängige Schnittstelle) verkabelt ist. Bei der MDI-Verkabelung überträgt der PC auf den Pins 1 und 2. Beim Hub, Switch, Router oder Access Point ist die Perspektive umgekehrt und der Hub empfängt auf den Pins 1 und 2. Diese Verkabelung wird als Media Dependant Interface-Crossover (MDI-X) bezeichnet.

14 Glossar

NAT

Network Address Translation. NAT befähigt alle Computer Ihres Netzwerks, eine IP-Adresse zu teilen. Die NAT-Eigenschaft des Routers ermöglicht Ihnen, auf das Internet von jedem Computer in Ihrem Heimnetzwerk aus zuzugreifen, ohne dass Sie mehrere IP-Adressen von Ihrem ISP erwerben müssen.

Netzwerk

Ein Netzwerk ist eine Gruppe von Computern und anderen Geräten, die miteinander verbunden sind, um Daten auszutauschen oder Ressourcen gemeinsam zu nutzen. Netzwerke können unterschiedlich groß sein. Einige befinden sich in einem einzigen Raum, andere umspannen Kontinente.

Network Interface Card (NIC)

Eine Netzwerkkarte, die in einem Gerät einer EDV-Anlage, zum Beispiel in einem Computer, eingebaut ist, ermöglicht es Ihnen, sich mit dem Netzwerk zu verbinden. Eine NIC ist auch als Adapter oder Adapterkarte bekannt.

Protokoll

Ein Regelpaket für die Kommunikation zwischen Geräten in einem Netzwerk. Die Regeln geben das Format, die Zeitintervalle, die Ablaufsteuerung und die Fehlersteuerung vor.

PSTN

Public Switched Telephone Network (Telefonfestnetz).

PPPoA

Point-to-Point-Protokoll über ATM. PPP über ATM ist ein Protokoll für die Verbindung von Remote-Hosts mit dem Internet über eine ständige Verbindung, indem eine Wählleitung simuliert wird.

PPPoE

Point-to-Point-Protokoll über Ethernet. Das Point-to-Point-Protokoll ist eine Datenübertragungsmethode, die ursprünglich für Wählverbindungen erstellt wurde; PPPoE kommt bei Ethernet-Verbindungen zum Einsatz.

RJ-45

Ein Standardstecker, der verwendet wird, um Ethernet-Netzwerke zu verbinden. „RJ" steht für "registered jack" (genormte Buchse).

Router

Ein Gerät, das als zentraler Hub agiert, indem es sich mit jeder Netzwerkschnittstellenkarte jedes Computers verbindet und den Datenverkehr zwischen dem lokalen Netzwerk und dem Internet verwaltet.

Server

Ein Computer in einem Netzwerk, der von mehreren Endgeräten gemeinsam genutzt wird. Server geben Endgeräten Zugriff auf gemeinsam genutzte Netzwerkdienste wie Computerdateien und Druckerwarteschlangen.

SSID

Service Set Identifier (Kennung eines Funknetzwerks). Einige Anbieter von drahtlosen Produkten verwenden SSID austauschbar mit ESSID.

14 Glossar

Subnetzadresse

Eine Erweiterung des IP-Adressierungskonzepts, die es ermöglicht, eine einzige IP-Netzwerkadresse für mehrere physikalische Netzwerke zu verwenden.

Subnetzmaske

Eine Subnetzmaske, die ein Teil der TCP/IP-Information sein kann, die von Ihrem ISP zur Verfügung gestellt wird, ist ein Satz mit vier Zahlen und wie eine IP-Adresse konfiguriert. Sie wird verwendet, um IP-Adresszahlen zu erstellen, die nur innerhalb eines bestimmten Netzwerks verwendet werden (im Gegensatz zu gültigen IP-Adresszahlen, die vom Internet erkannt werden und durch InterNIC zugeteilt werden müssen).

Subnets

Ein Netzwerk, das Bestandteil eines größeren Netzwerks ist.

Switch

Ein Gerät, das verschiedene LANs miteinander verbindet, um ein einziges logisches LAN zu bilden, das aus verschiedenen LAN-Teilen besteht. Switches sind vergleichbar mit Brücken, da sie LANs verschiedener Arten miteinander verbinden. Jedoch verbinden sie mehr LANs als eine Brücke und sind im Allgemeinen ausgereifter.

TCP/IP

Transmission Control Protocol/Internetprotokoll. Dies sind die Bezeichnungen für zwei der bekanntesten Protokolle, die für die Zusammenschaltung von Netzwerken entwickelt wurden. Ursprünglich ein UNIX-Standard, wird TCP/IP mittlerweile von fast allen Plattformen unterstützt und ist das Protokoll des Internets.

TCP

Bezieht sich auf den Inhalt von Daten, die durch ein Netzwerk übertragen werden und stellt sicher, dass die gesendeten Daten vollständig am Bestimmungsort ankommen. IP bezieht sich auf die Adresse der Endgeräte, an die die Daten gesendet werden, sowie auf die Adresse des Zielnetzwerks.

Datenverkehr

Die Bewegung von Datenpaketen in einem Netzwerk.

Universal plug and play

Universal plug and play ist ein System, das es kompatiblen Anwendungen ermöglicht, einige ihrer Einstellungen vom Router zu lesen. So können automatisch einige oder alle ihrer Einstellungen konfiguriert werden, so dass der Nutzer weniger Konfigurationen vornehmen muss.

URL-Filter

Ein URL-Filter ist die Eigenschaft einer Firewall, die seine Clients daran hindert ,auf bestimmten Webseiten zu surfen.

UTP

Unshielded Twisted-Pair (ungeschirmte Kabel mit verdrillten Adernpaaren) sind die Kabel, die von 10BASET und 100BASE-Tx-Ethernet-Netzwerken verwendet werden.

14 Glossar

VCI

VCI – virtuelle Kanalermittlung. Die Kennzeichnung im ATM(Asynchroner Transfermodus)-Zellen-Header, die ermittelt, zu welchem virtuellen Kanal die Zelle gehört.

VPI

VPI – virtuelle Pfadermittlung. Das Feld im ATM(Asynchroner Transfermodus)-Zellen- Header, das ermittelt, zu welchem VP (virtuellen Pfad) die Zelle gehört.

WAN

Wide Area Network (Fernnetz). Ein Netzwerk, das Computer, die an unterschiedlichen Standorten stehen, miteinander verbindet (zum Beispiel in verschiedenen Gebäuden, Städten oder Ländern). Das Internet ist ein solches Fernnetz.

WEP

Wired Equivalent Privacy. Ein gemeinsam genutzter Verschlüsselungsmechanismus für die drahtlose Vernetzung. Die Verschlüsselungsstärke beträgt 40/64 bit oder 128 bit.

Wi-Fi

Wireless Fidelity. Die ist das Zertifikat, das von WECA für Produkte ausgestellt wird, welche die Kompatibilitäts-Kriterien erfüllen (siehe auch 802.11b, WECA).

Wi-Fi Alliance

Die Wi-Fi Alliance ist eine Handelsgruppe, welche die Wi-Fi-Handelsmarke besitzt, die Kompatibilität von Produkten testet und bescheinigt und die Technologie fördert.

Drahtloser Client

Mit diesem Begriff wird ein Desktop oder mobiler PC beschrieben, der drahtlos mit Ihrem Drahtlosnetzwerk verbunden ist.

Wireless LAN Service Area

Ein anderer Begriff für ESSID (Extended Service Set Identifier)

Wizard

Eine Windows-Anwendung, die Vorgehensweisen wie die Installation oder Konfiguration automatisiert.

WLAN

Wireless Local Area Network (drahtloses lokales Netzwerk). Ein WLAN ist eine Gruppe von Computern und Geräten, die drahtlos in einem relativ kleinen Bereich (zum Beispiel in einer Wohnung oder einem Büro) miteinander verbunden sind.

WPA

Wi-Fi Protected Access (geschützter Zugang). Ein dynamisch wechselnder Verschlüsselungsmechanismus für die drahtlose Vernetzung. Die Verschlüsselungsstärke liegt bei 256 bit.

Der Umwelt zuliebe. Telekom Austria

Infos unter 0800 100 100 und www.telekom.at

Vorbehaltlich Satz- und Druckfehler.
Stand: Mai 2011.

TELE KOM AUS TRIA